Actuaries Institute.

Quantum Computing for Actuaries

Presented by
the Actuaries Institute and
Quantum Australia
28 July 2026

The Actuaries Institute acknowledges the traditional custodians of the lands and waters where we live and work, travel, and trade.

We pay our respect to the members of those communities, Elders past and present, and recognise and celebrate their continuing custodianship and culture.

Actuaries Institute.

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Hermann	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

Actuaries Institute.

Q&A

Join at
slido.com
#2008252

Important notice for all participants

This meeting is being conducted in accordance with Institute's Code of Conduct and attended by members in their professional capacity.

It is acknowledged that professional members in their employed capacity, may be active market participants in their respective industries who may compete with each other as defined by competition law.

Participants are, therefore, reminded that in accordance with their competition law compliance obligations they should not:

- discuss any matter that may be perceived as being cooperation by competitors in a market to influence that market;
- discuss any matters that could be regarded as fixing, maintaining or controlling prices, allocation of customers or territories, coordinating bids and/or restricting output or acquisitions in any circumstances;
- share commercially sensitive information relating to their employer; or
- share information for an anti-competitive purpose.

Actuaries Institute.

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Hermann	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

Actuaries Institute.

Quantum Australia

National mandate and why quantum matters for industry

Translating Capability Strengths into Quantum Industry Growth

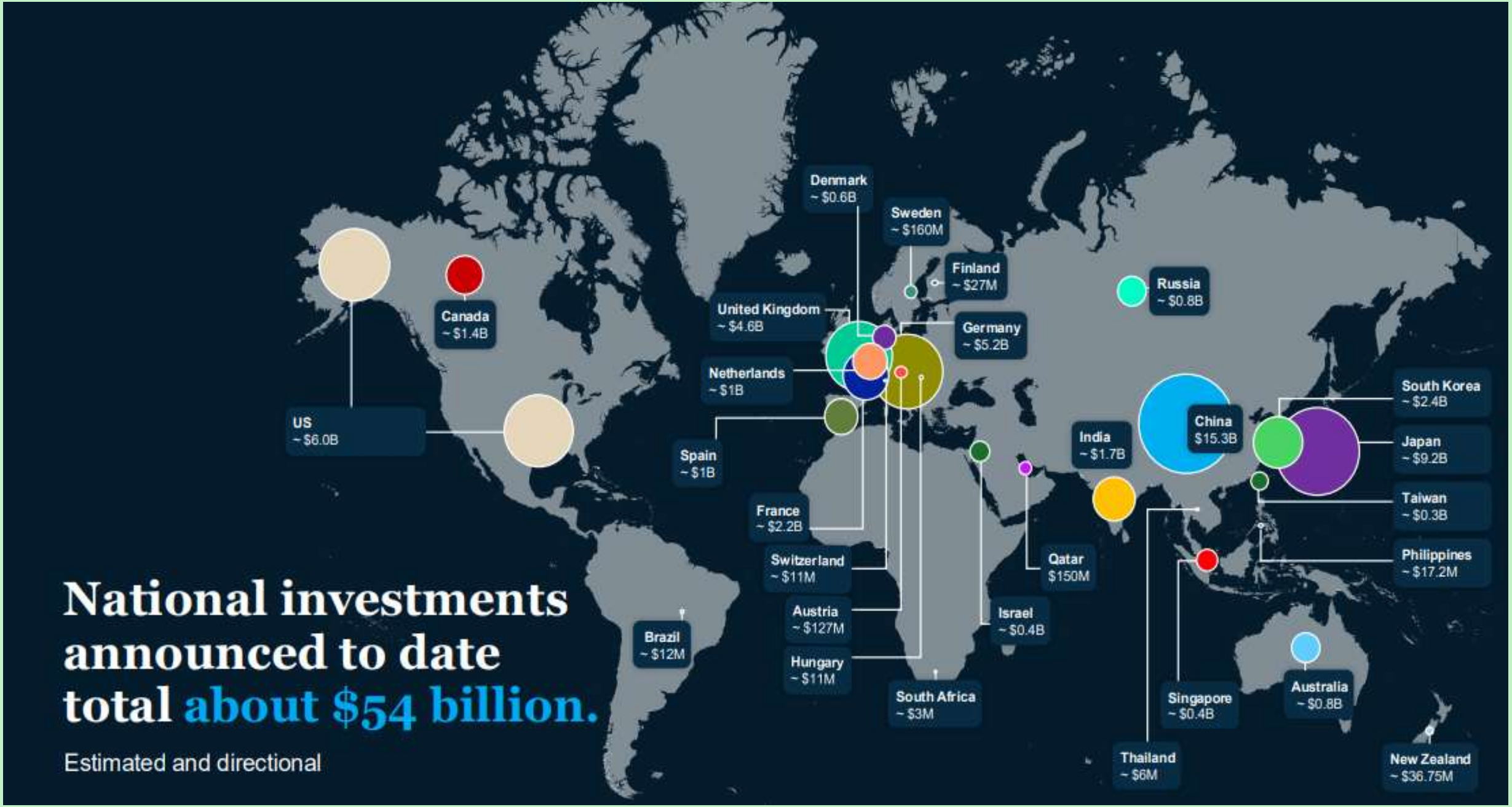

Denmark
~ $0.6B
Sweden
~ $160M
Finland
~ $27M
Russia
~ $0.8B
Canada
~ $1.4B
United Kingdom
~ $4.6B
Germany
~ $5.2B
Netherlands
~ $1B
US
~ $6.0B
Spain
~ $1B
India
~ $1.7B
China
$15.3B
South Korea
~ $2.4B
Japan
~ $9.2B
Taiwan
~ $0.3B
France
~ $2.2B
Switzerland
~ $11M
Qatar
$150M
Philippines
~ $17.2M
Austria
~ $127M
Israel
~ $0.4B
Brazil
~ $12M
Hungary
~ $11M
South Africa
~ $3M
Singapore
~ $0.4B
Australia
~ $0.8B
Thailand
~ $6M
New Zealand
~ $36.75M
National investments announced to date total about $54 billion.
Estimated and directional

TABLE A: QUANTUM CLUSTERS RANKING

Rank	Quantum Cluster	Country	Region	Dimension Rankings		
				Market Orientation	Collaboration Intensity	Ecosystem Maturity
1	Cambridge	UK	UK, Canada, and Australia	2-	11-	2
2	Greater Helsinki	Finland	EU	2-	15	4
3	Oxford	UK	UK, Canada, and Australia	8	5	3
4	San Francisco Bay Area	US	US	1	11-	8-
5	Greater Glasgow	UK	UK, Canada, and Australia	16-	4	5
6	Tel Aviv Metropolitan Area	Israel	Rest of the World	6	19	7
7	Karlsruhe	Germany	EU	20-	2-	6
8	Hefei	China	China	4-	6-	24-
9	Denver–Boulder Region	US	US	4-	28-	15-
10	Greater Geneva Bern Area	Switzerland	Rest of the World	12	6-	15-
11	Bristol–Bath Region	UK	UK, Canada, and Australia	20-	23-	1
12=	Canberra	Australia	UK, Canada, and Australia	9	25-	11
12=	Toronto–Waterloo Corridor	Canada	UK, Canada, and Australia	10	31	8-
14=	Greater Boston	US	US	11	32	14
14=	London Commuter Belt	UK	UK, Canada, and Australia	16-	10	23
16	Greater Copenhagen	Denmark	EU	26	6-	13
17	Greater Sydney	Australia	UK, Canada, and Australia	15	21	19
18	Greater Washington	US	US	7	17	31
19	Metro Vancouver	Canada	UK, Canada, and Australia	14	35	20
20	Greater Paris	France	EU	13	33	24-
21	Greater Austin	US	US	20-	27	27
22	Munich Metropolitan Area	Germany	EU	18	40	22

A quantum cluster is a concentrated ecosystem meeting two minimum thresholds:

- **Funding:** 2+ startups with $10M+ combined, or 1 startup with $25M+
- **Institutions:** 5+ research, industry, or government bodies actively engaged in quantum

Source: **European Centre for International Political Economy**

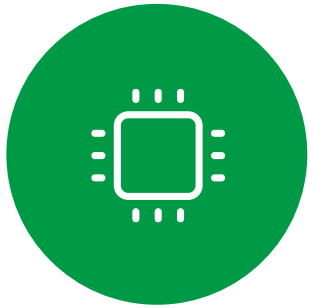
Australia’s National Quantum Strategy (2023)

Vision: In 2030, Australia is recognised as a leader of the global quantum industry, and quantum technologies are integral to a prosperous, fair and inclusive Australia

Thriving research and development, investment in and use of quantum technologies.

A skilled and growing quantum workforce.

Standards and frameworks that support national interests.



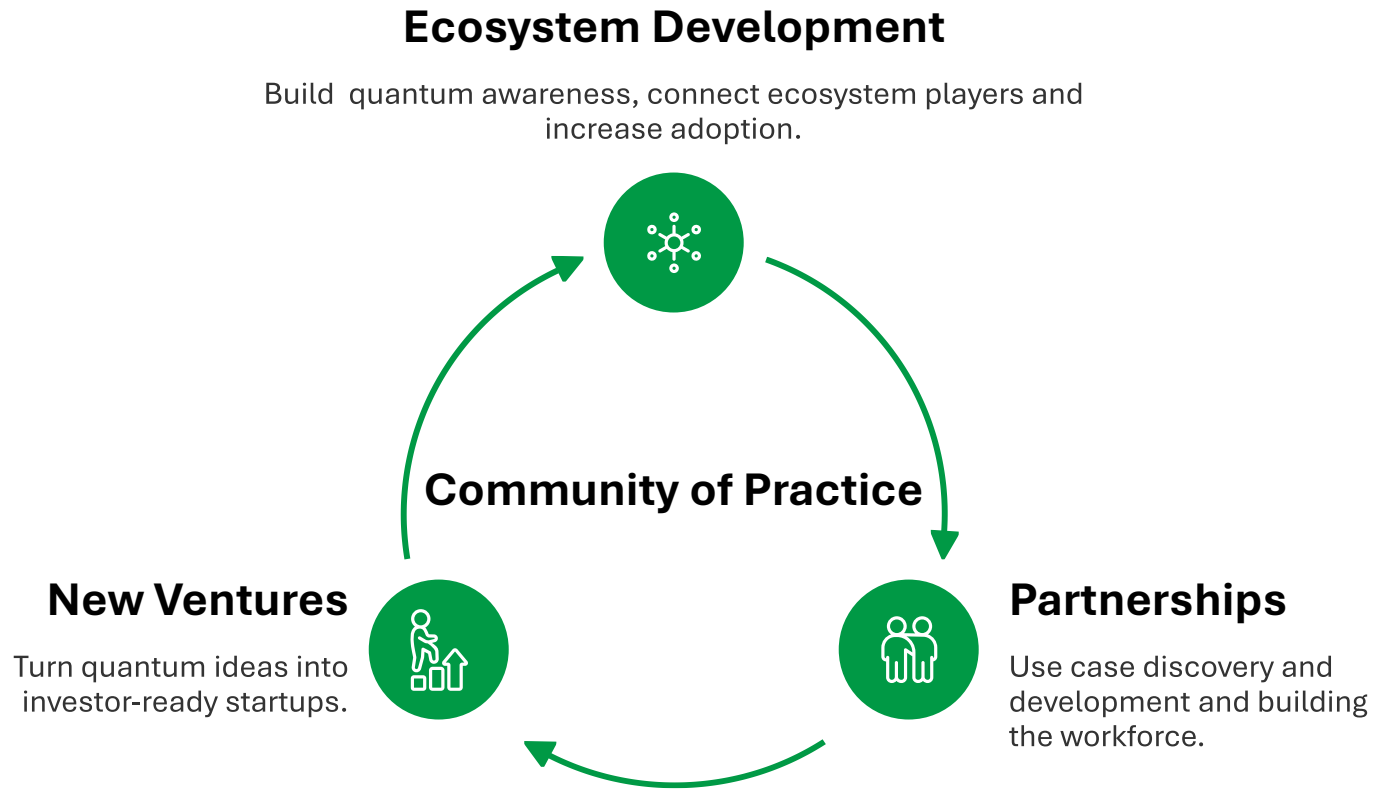
Securing access to essential quantum infrastructure & materials.

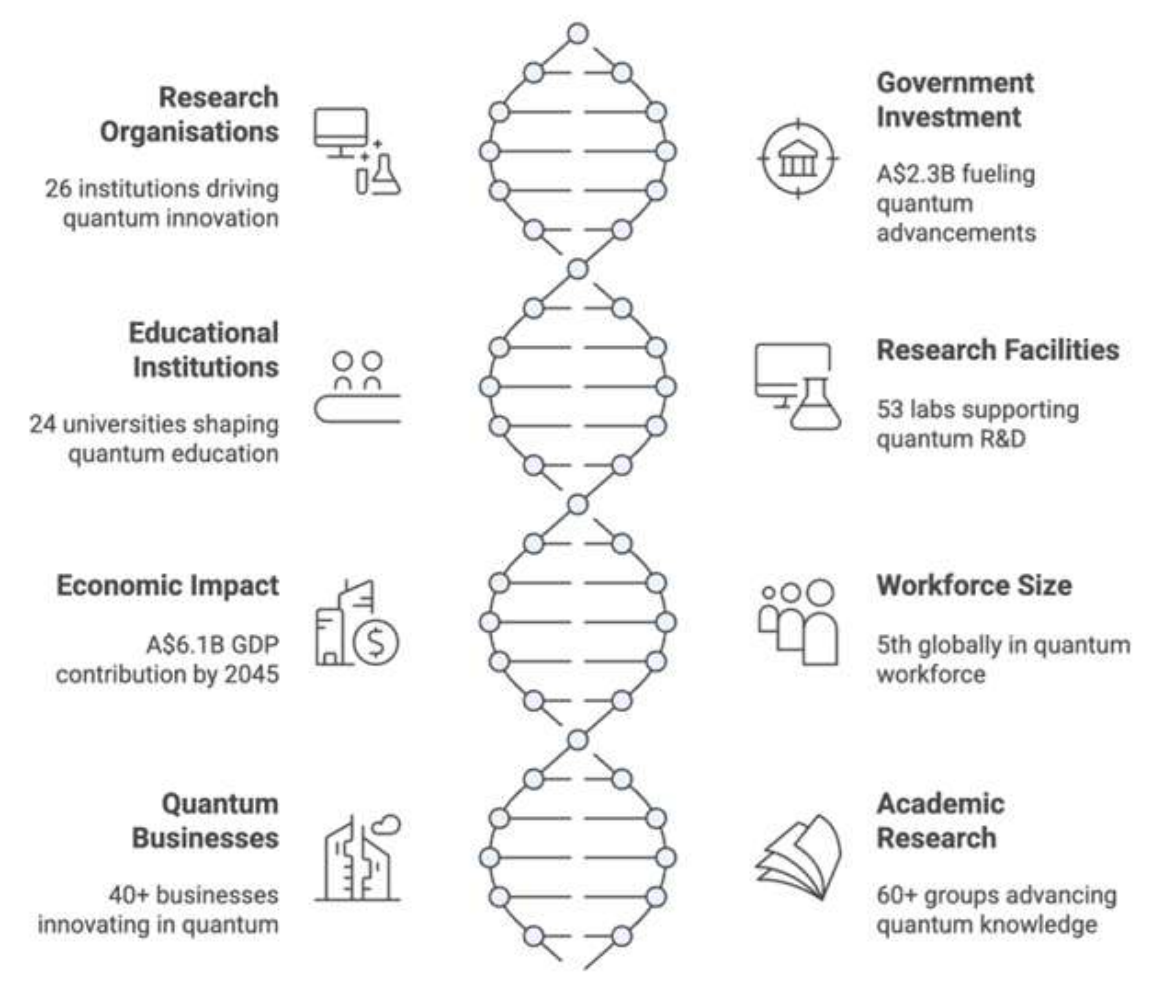
A trusted, ethical and inclusive quantum ecosystem.

What is Quantum Australia?

The National Centre for Quantum Growth (2024)

Founded in 2024 as a partnership between 13 Universities, federal (DISR) and state governments, industry and key stakeholders leading the growth of Australia's quantum ecosystem





Where we are today

A$**2.3B public funding** in fundamental research over the past 25 years

- **26 leading research orgs & 60+ academic** groups driving quantum breakthroughs
- **24 universities & 53 world-class labs** powering advanced R&D
- **Top 10 globally for quantum talent capacity**
- **3 active CoE** with quantum mandate (**2 new**)
  - ARC Centre of Excellence for Quantum Computer Performance and Integration
  - ARC Centre of Excellence in Quantum Cybersecurity
- **40+ quantum businesses** - many founded in the last five years and more to come

Australia’s Quantum Sector

Selected highlights across quantum **computing, sensing, communications**, and **supply chain**

Cybersecurity & QKD

QuintessenceLabs secures A$20M funding round led by A$15M NRF (Australia’s A$15b government fund) to scale quantum cybersecurity globally.

Diamond Quantum Foundry

Quantum Brilliance receives A$13M NRF + A$10M Breakthrough Victoria/state gov fund to establish Australia’s first diamond-based quantum foundry.

Quantum Control Leadership

Global Quantum control leader Q-CTRL secured world’s largest quantum Series B (US $113M), partners with IBM Quantum, and demonstrates quantum advantage in navigation trials

Utility-Scale Compute Pathways

Silicon Quantum Computing (SQC) and Diraq selected for **DARPA Quantum Benchmarking Initiative**, advancing fault-tolerant, utility-scale systems by 2033.

Diraq secures $53M (US$38M) with the **US DoC CHIPS program** for its ‘quantum dot’ tech to be scaled and manufactured in the US.

Mega-Scale Ambition

PsiQuantum advances 1M-qubit system near Brisbane (~A$1B project, now well underway).

Cryo Engineering at Scale

Emergence Quantum, recently backed by Serendipity Capital, combines hardware-agnostic quantum engineering and cryogenic computing expertise to enable quantum, semiconductor and cryogenic infrastructure ventures scale.

New Ventures

Companies created since 2025 **17**

NewQ

Tailored for quantum entrepreneurs.

- 8-week online program
- Teams of 2-4, based in Australia
- ~8-hour commitment per week.
- Test your idea and build your pitch.
- Learn directly from experts, entrepreneurs, mentors, and business leaders.

NextQ

Quantum venture creation.

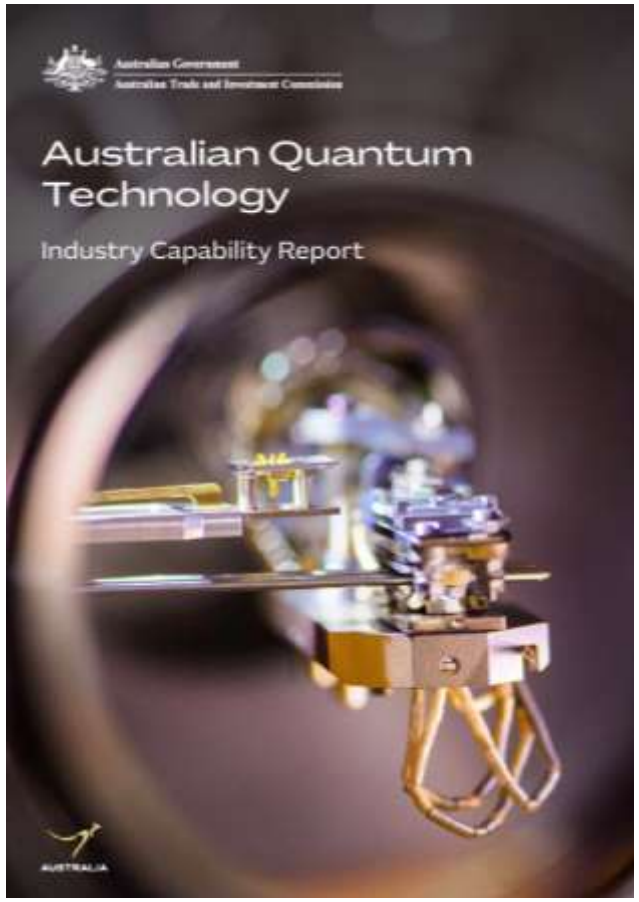
- Start your quantum business.
- 20-week bespoke support.
- Connect with industry & investors.
- Dedicated entrepreneurial help and business support.
- Support with commercial and investor readiness.

Quantum Australia

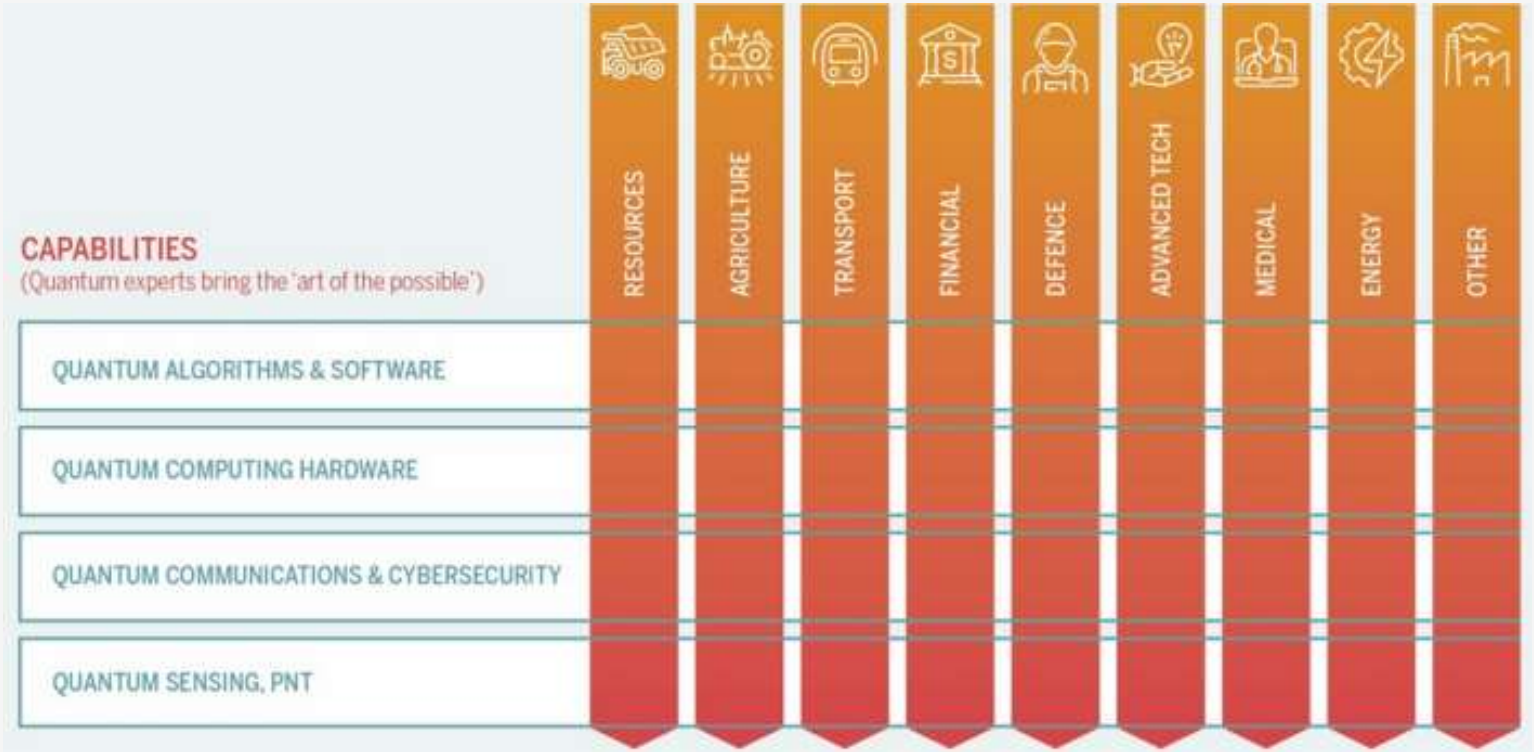
Register for NewQ: **quantum-australia.com/newqform**

Industry Capability Report

Austrade &
Quantum Australia



QA actively provides support to all quantum verticals engaging with end-users across multiple sectors.



Quantum for actuaries: risk now, opportunity later

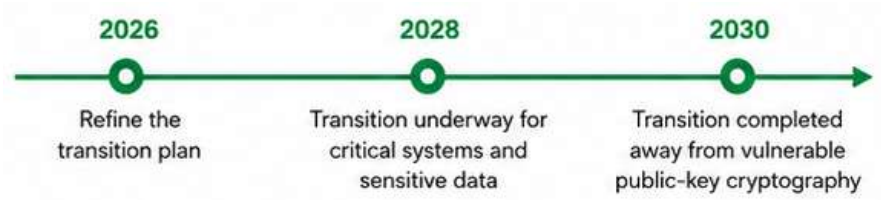
Cryptography is the immediate priority; modelling applications are longer-term.

01

Cryptography risk comes first

Organisations should prepare before capable quantum computers arrive.

- **The issue**
  Future quantum computers could compromise widely used public-key cryptography. PREVENT - '*Q-Day*' & '*Harvest now, decrypt later*'.
- **Why insurers care**
  Policyholder, claims, health and financial data can remain sensitive for decades.
- **Actuarial contribution**
  Quantify the financial exposure and consider it in Financial Condition Reports (FCRs), risk appetite and affected insurance products.



02

Opportunity spans actuarial sectors

Focus on valuable modelling problems, not quantum for its own sake.

- **Insurance & reinsurance**
- **Superannuation & investments**
- **Health & longevity**
- **Climate & catastrophe risk**
- **Government & infrastructure**

Potential value

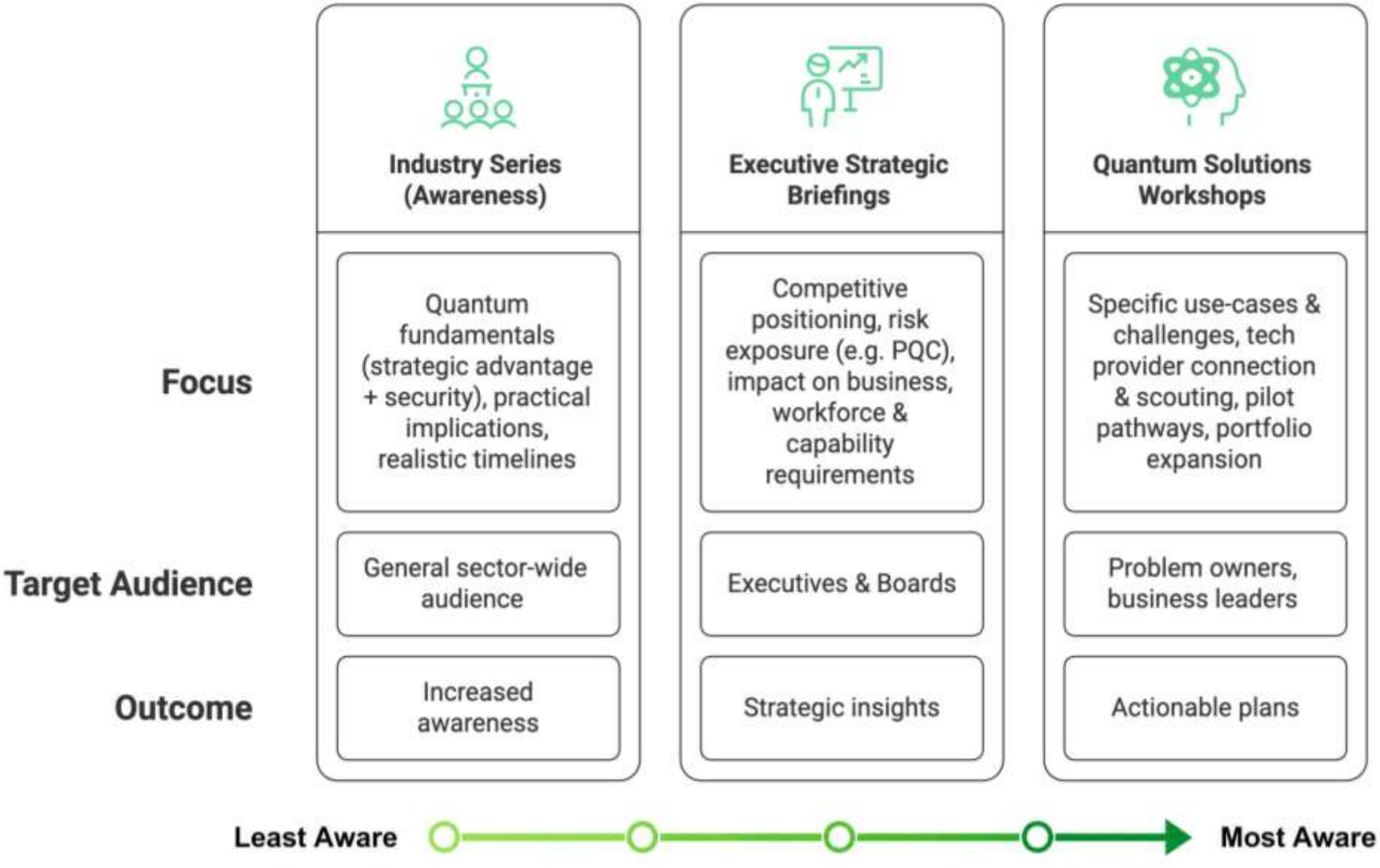
Richer scenarios, faster optimisation and more complex models, where today's methods reach practical limits.

Reality check: quantum is not yet delivering broad, production-scale business value.

Practical message: prepare for cryptography risk now; identify one or two valuable problems to explore.

Sources: Actuaries Institute (Introduction to Quantum Computing; FCR quantum risk, 2026); NIST.

We help end-users move from awareness to adoption through structured pathways



Quantum Australia Conference

17-18 Feb 2027 | Sydney - Canberra

Stay connected.

Quantum Australia

queries@quantum-australia.com

Quantum Australia

Subscribe to the Quantum Australia newsletter

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Hermann	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

Actuaries Institute.

Quantum 101

Dr Maja Cassidy

Deputy Director
ARC Centre of Excellence for Quantum Computer Performance and Integration

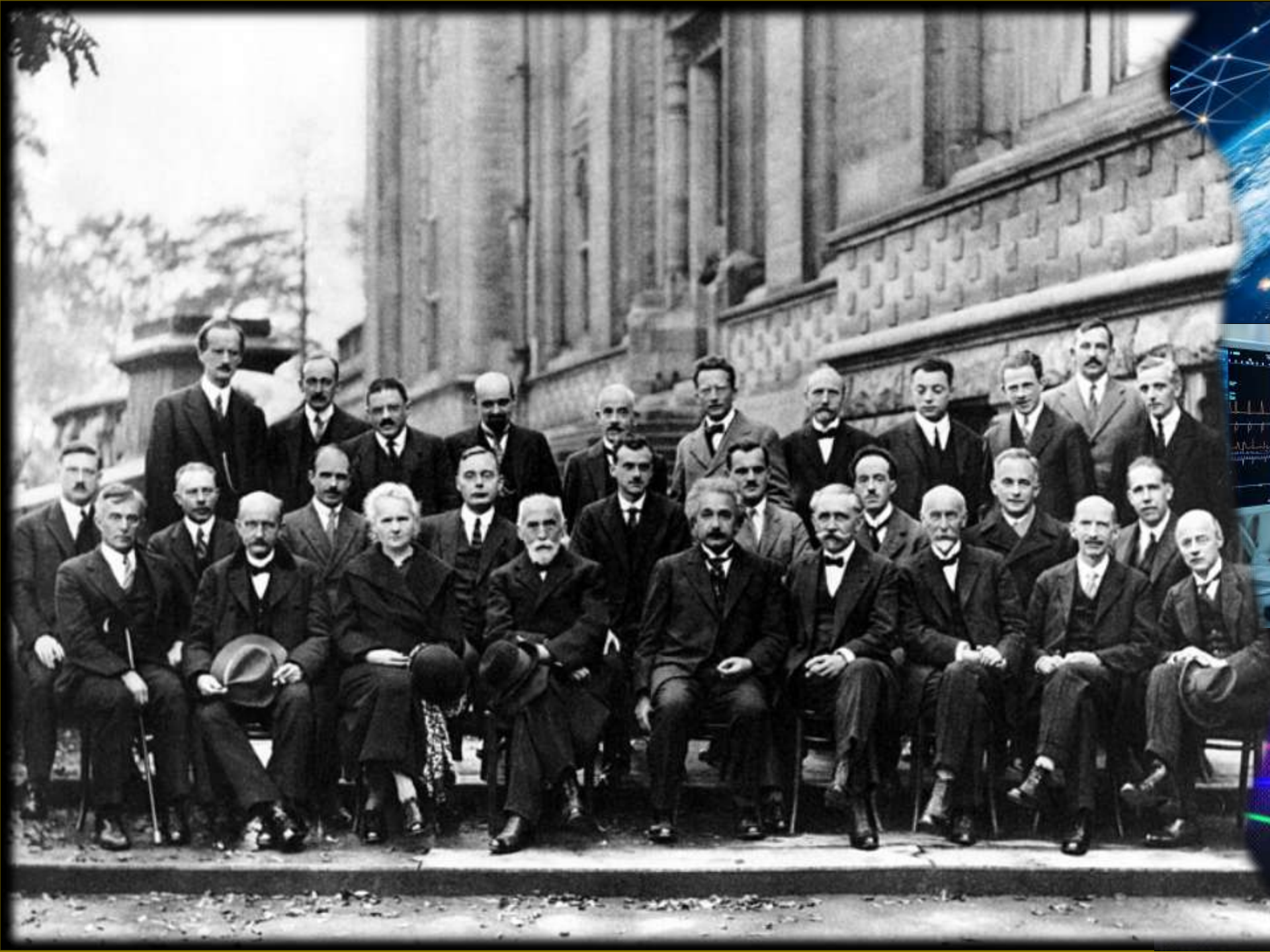
Actuarial Institute of Australia 28th July 2026

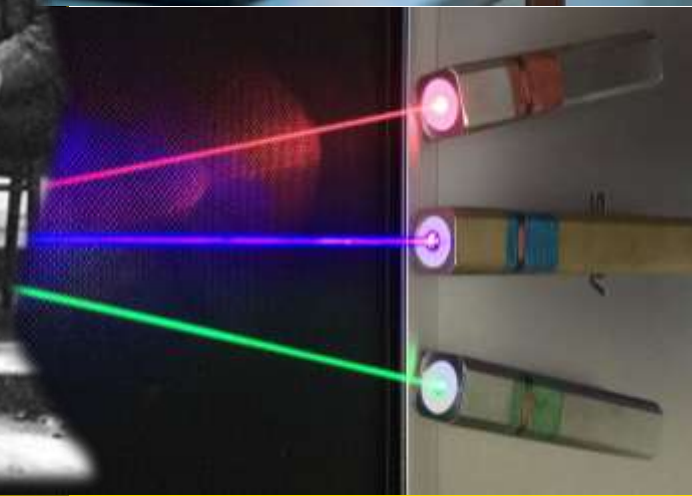
Quantum mechanics

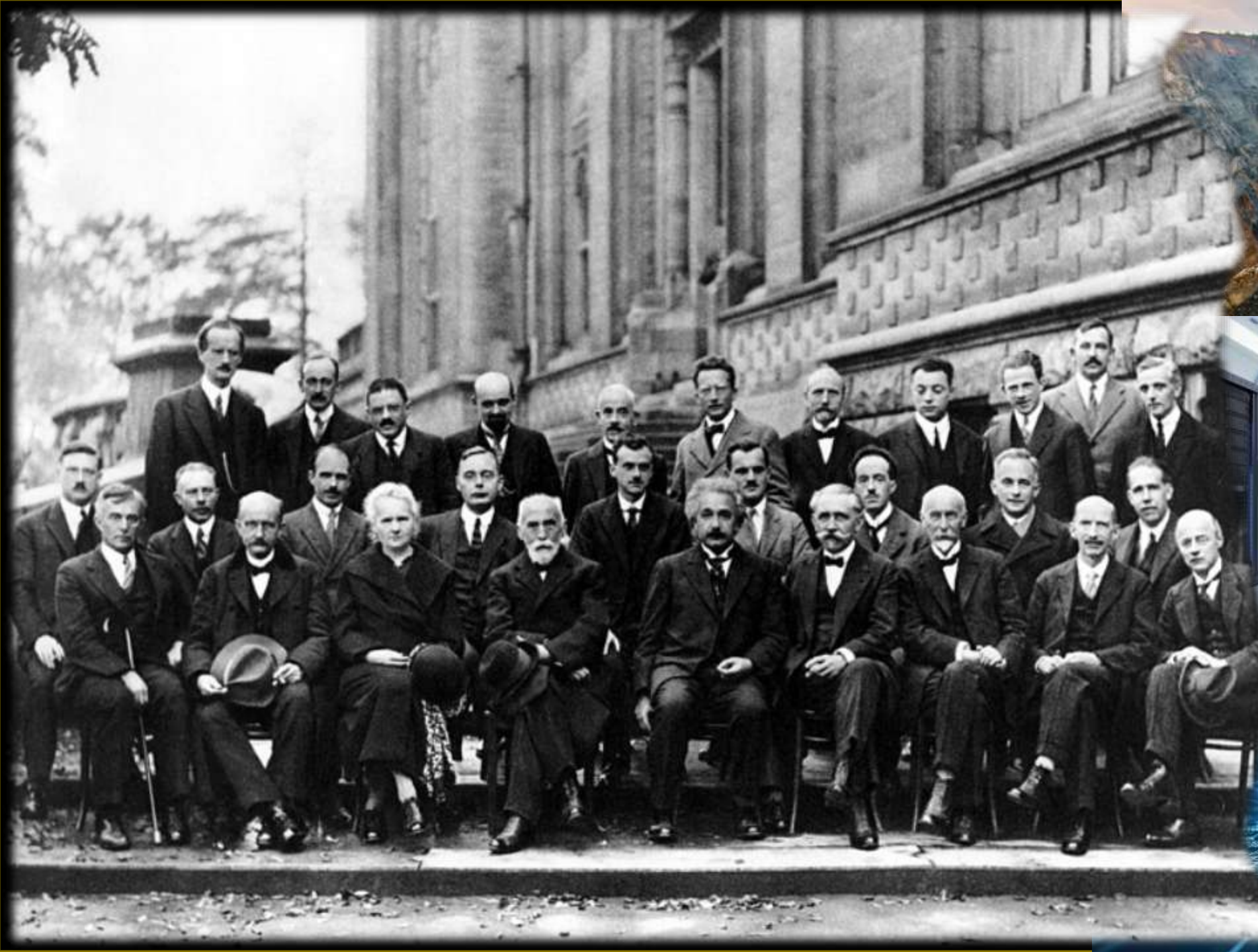
The laws of nature at the nanometre scale are quantum!

UNSW SYDNEY 75 YEARS

Image: Public Domain Pictures







Quantum superposition

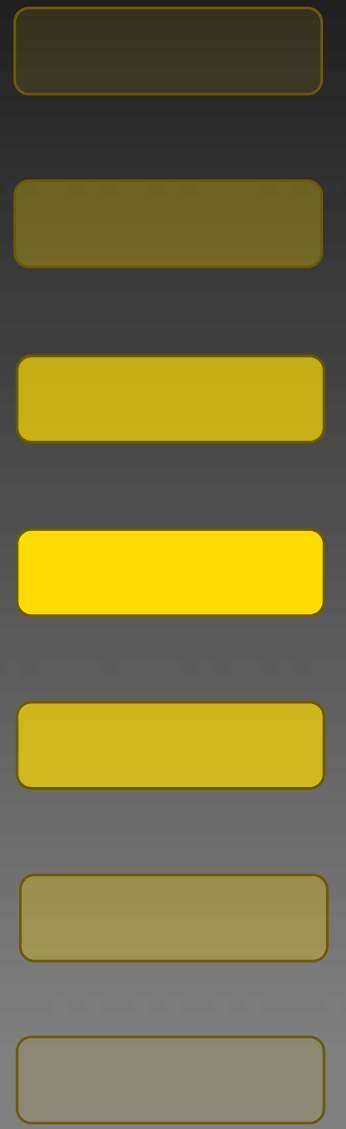
1

0

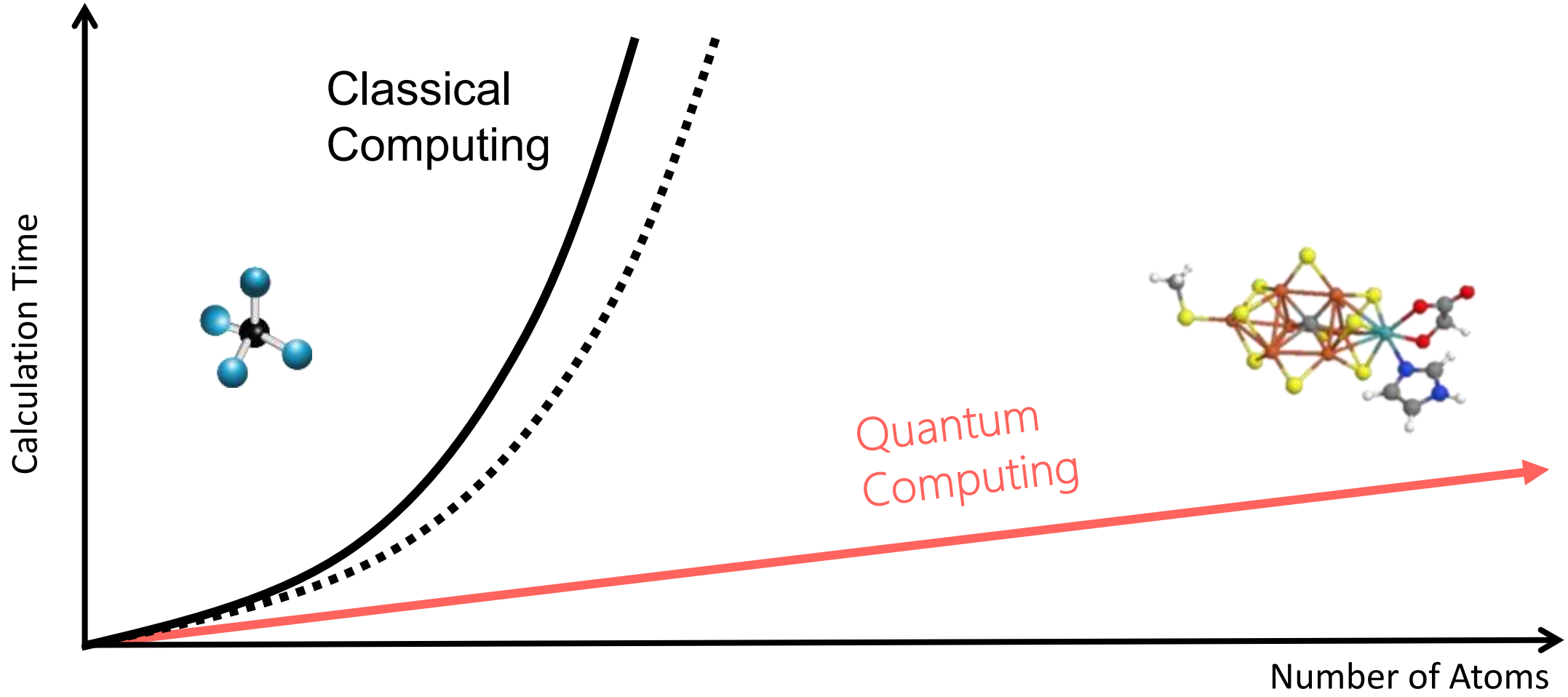
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

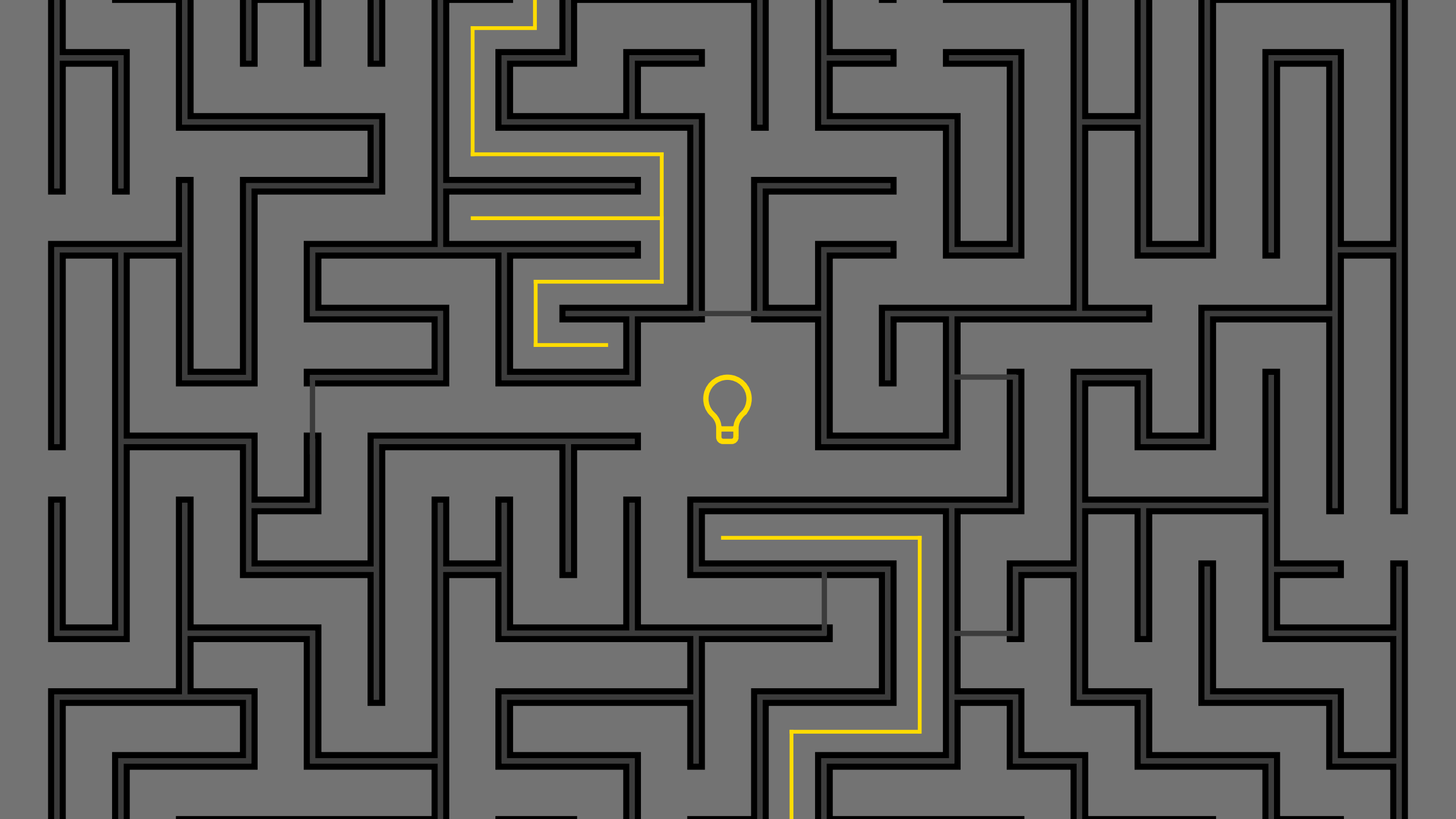
Quantum entanglement

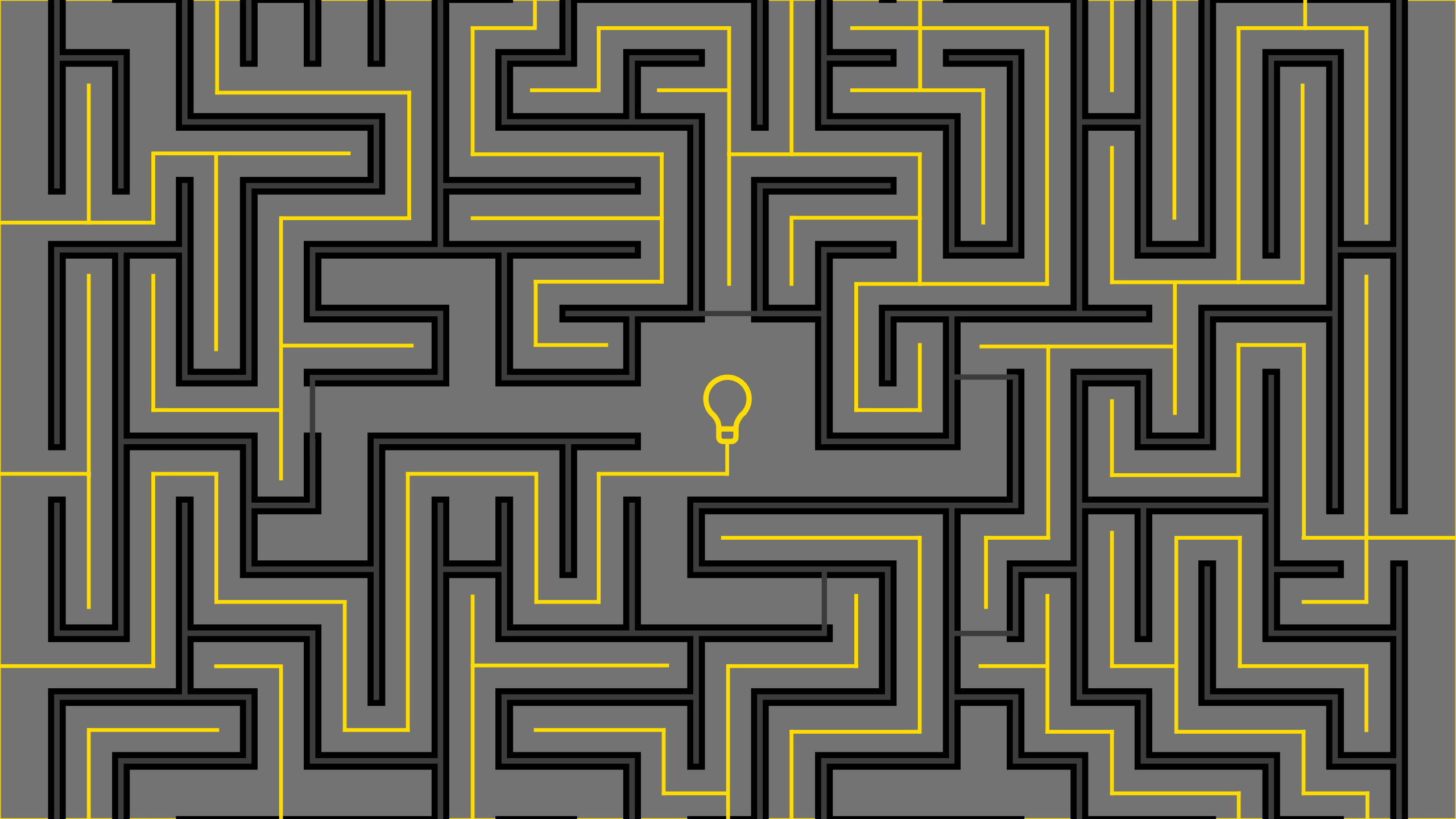
Quantum interference



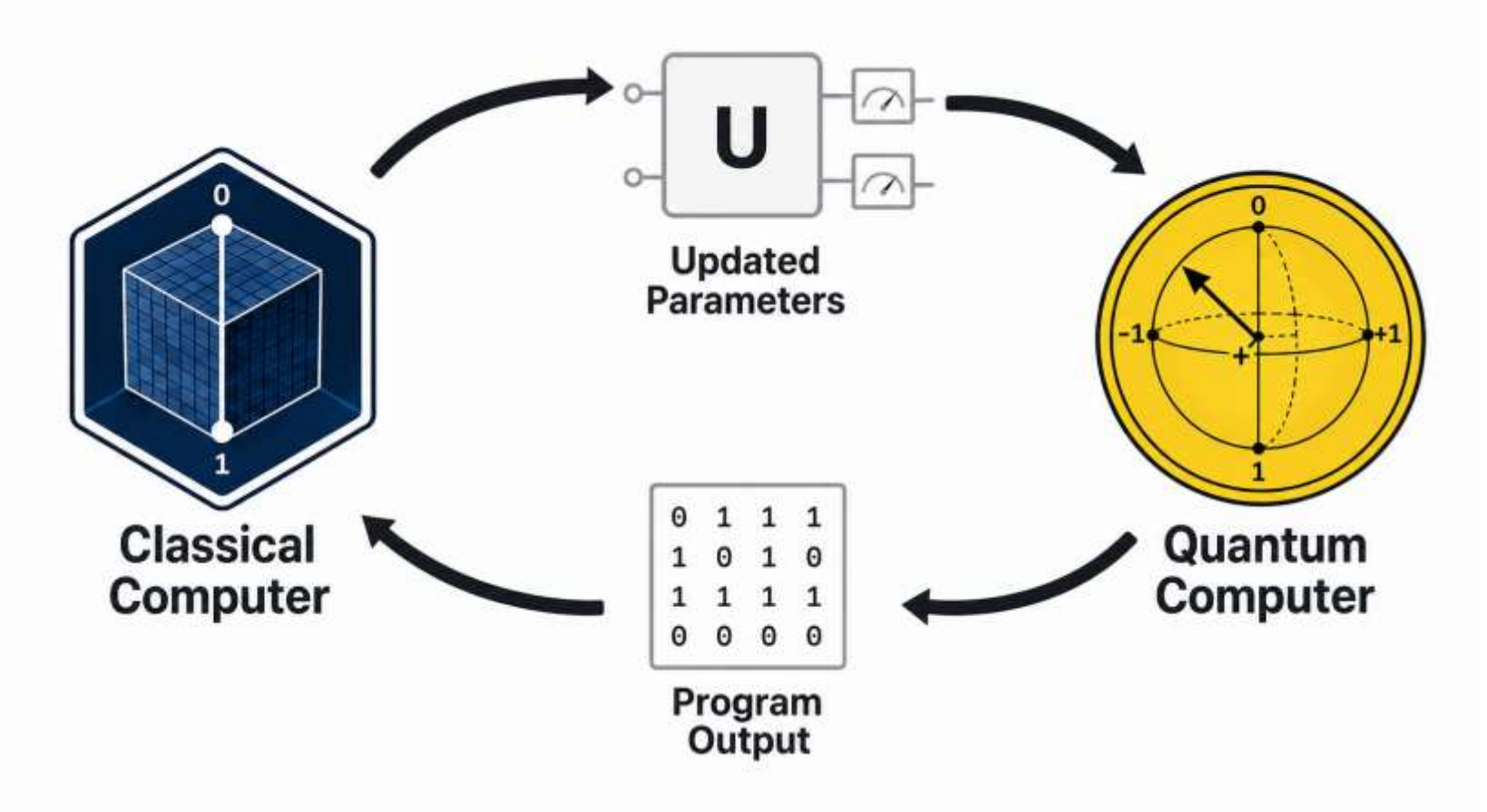
Quantum computers offer the potential of exponential speed up



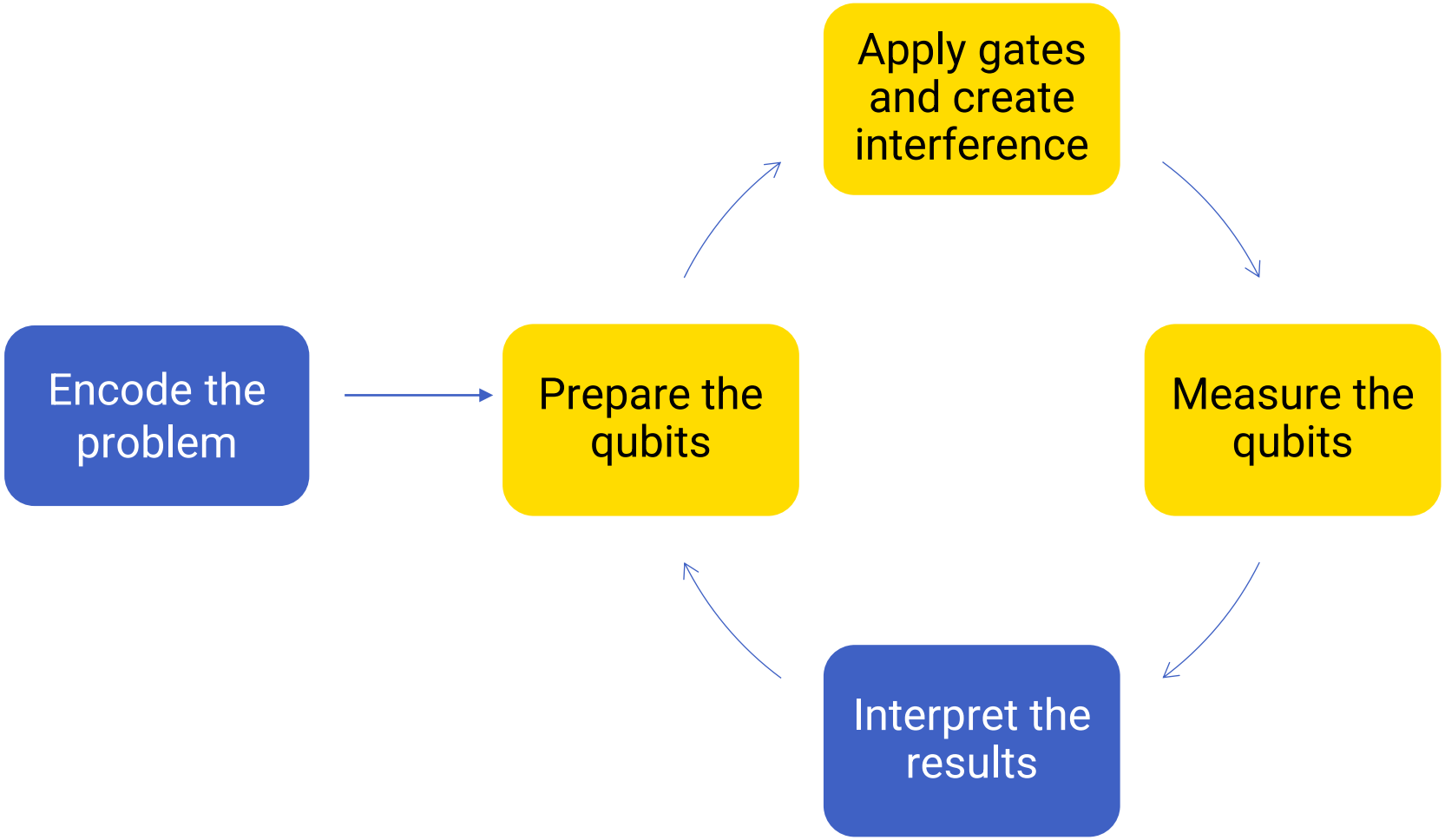




How a quantum algorithm runs



How a quantum algorithm runs



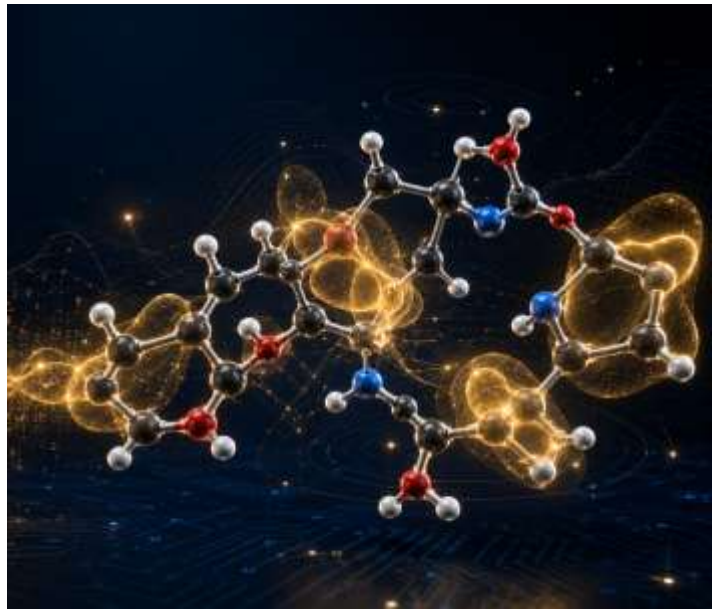
What sort of problems is a quantum computer good for?

- **Computationally complex -** The number of possible solutions or system states grows extremely rapidly with problem size.
- **Information sparse -** The calculation may involve an enormous state space, but the required input and output is a small number of values
- **Highly structured -** The problem contains mathematical patterns that a quantum algorithm can exploit through interference.
- **Probabilistic or sampling-based -** The desired result is an expectation value, probability, distribution or representative sample.
- **Expensive enough to justify the overhead -**Any speed-up must exceed the costs of data preparation, error correction, measurement and classical processing.

Possible applications of quantum computers

Factoring

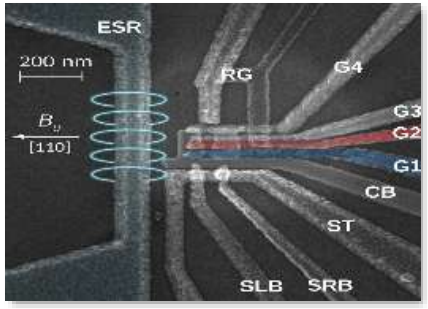
Optimization



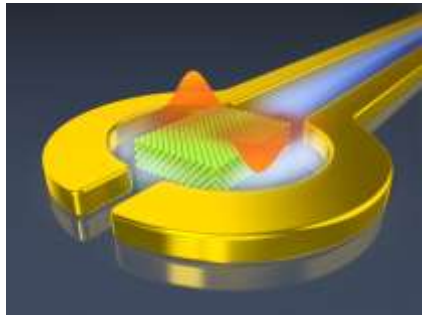
Chemistry & Materials

Many different qubit platforms

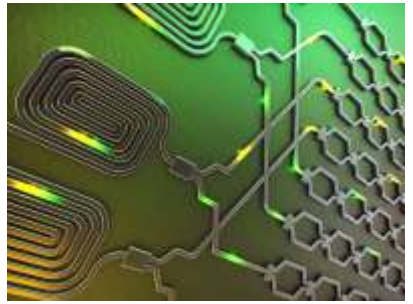
MOS Spin qubits
(UNSW, Delft, Rochester, Princeton, Intel, RIKEN, Diraq, HRL, Quantum Motion)



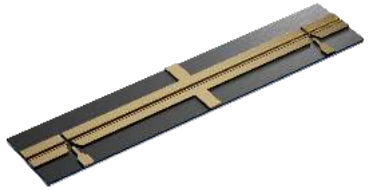
Noble Gas
(Princeton, Stanford, Argonne, UNSW, Tokyo, EeroQ)



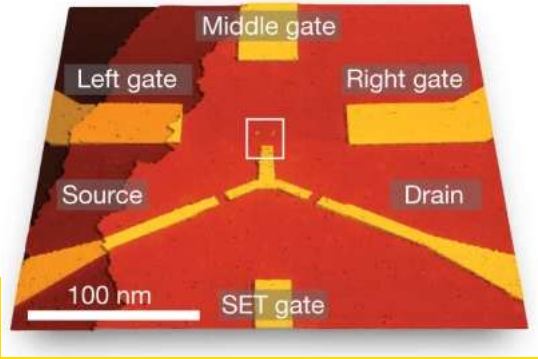
Photonic Qubits
(UQ, Bristol, Xanadu, PsiQuantum)



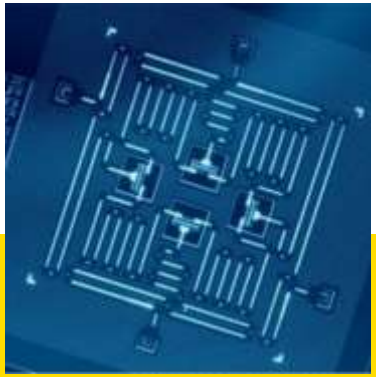
Topological Qubits
(Delft, Microsoft)



Donor Qubits
(UNSW, SQC)

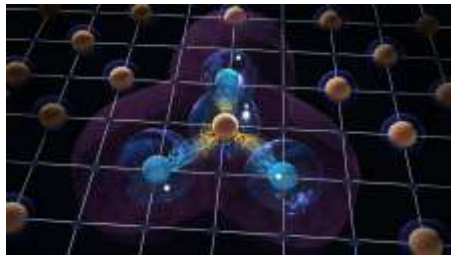


Superconducting Qubits
(Yale, UCSB, Zurich, Delft, Stanford, Princeton, Alice & Bob, Google, Rigetti, IBM, Amazon, OQC…)

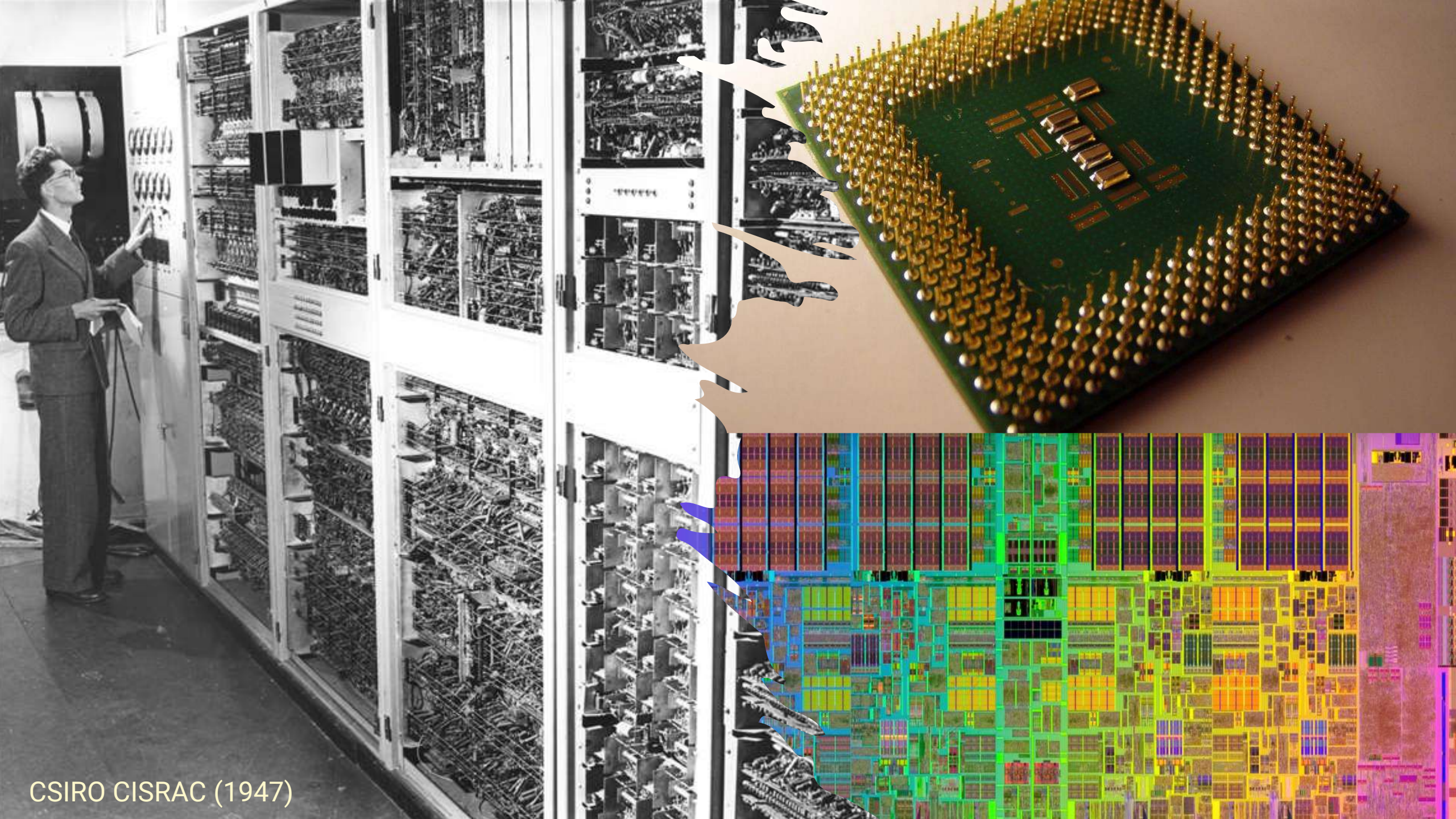


Ion Traps
(Harvard, MIT, Innsbruck, AQT, Quantinuum, IonQ, NIST…)

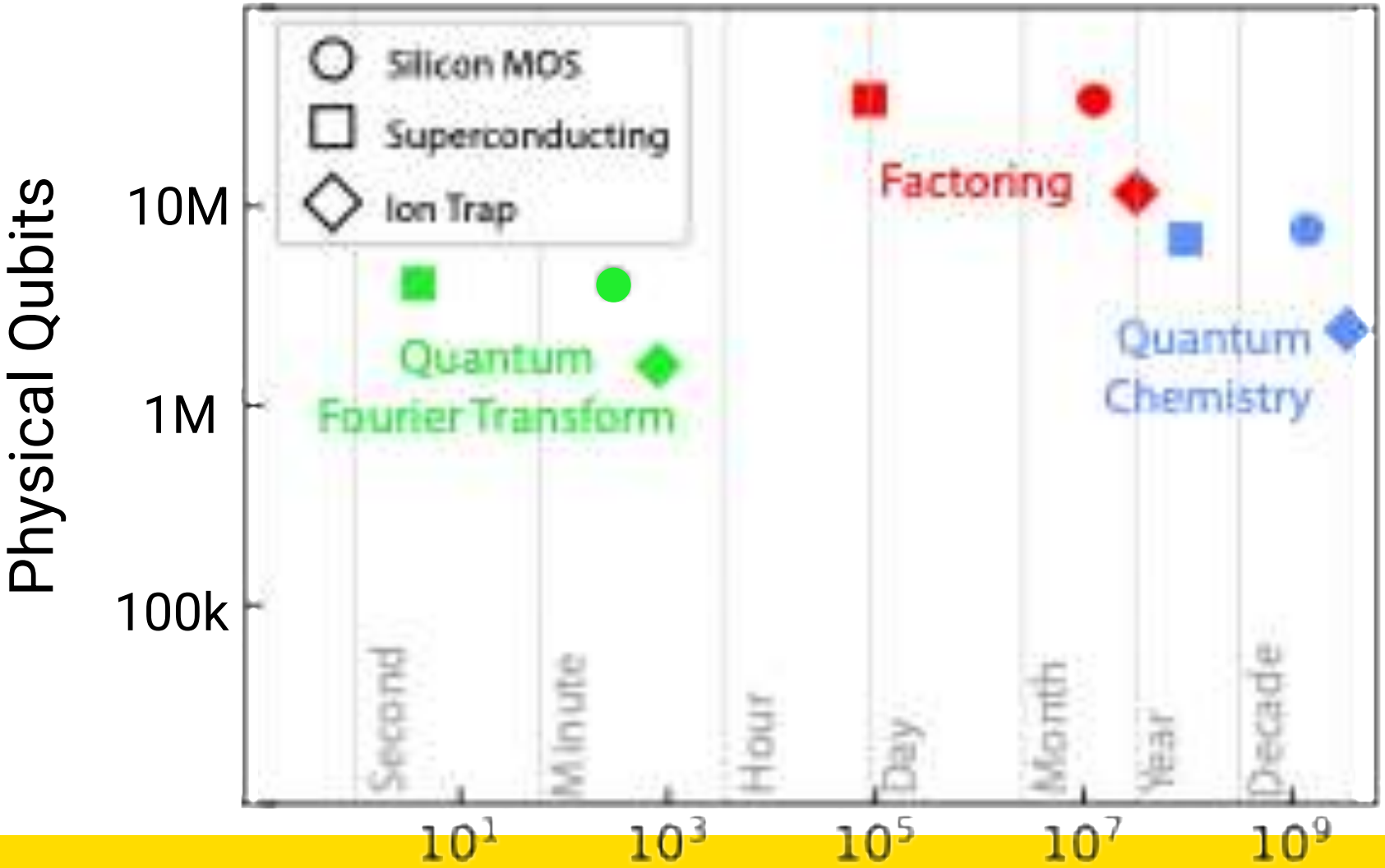
Rydberg Atom
(Harvard, Princeton,QuEra)



UNSW SYDNEY

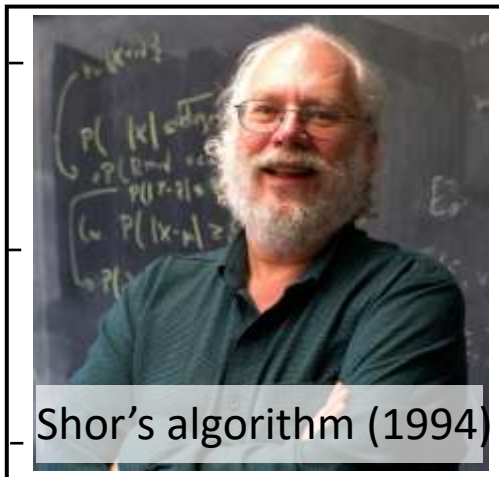

CSIRO CISRAC (1947)

Runtimes for quantum computing applications



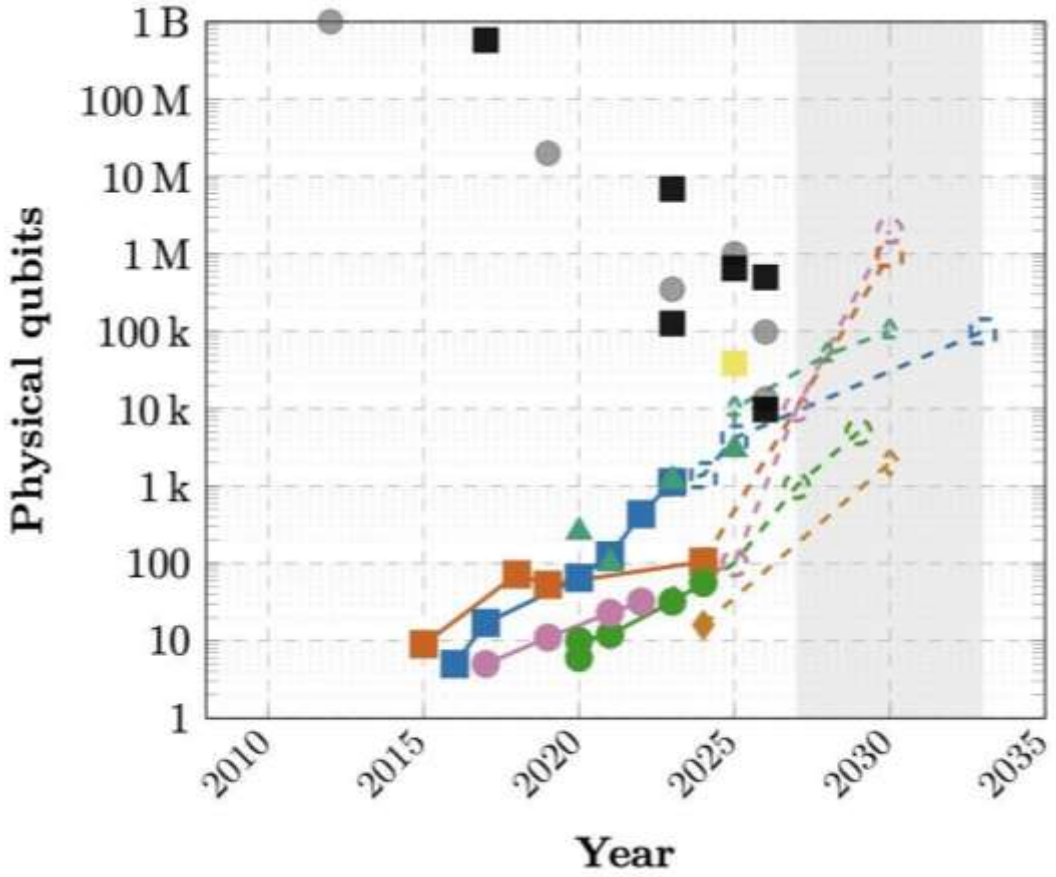
Microsoft quantum resource estimator (2024)

Industry pushing to large scale quantum computers


Shor's algorithm (1994)


PsiQuantum Brisbane

Advances in error correction bring required qubit count down



These algorithms require non-local connectivity

Alg. RSA-2048
IBM
Quantinuum

Alg. ECC-256 (lit.)
Google
IonQ

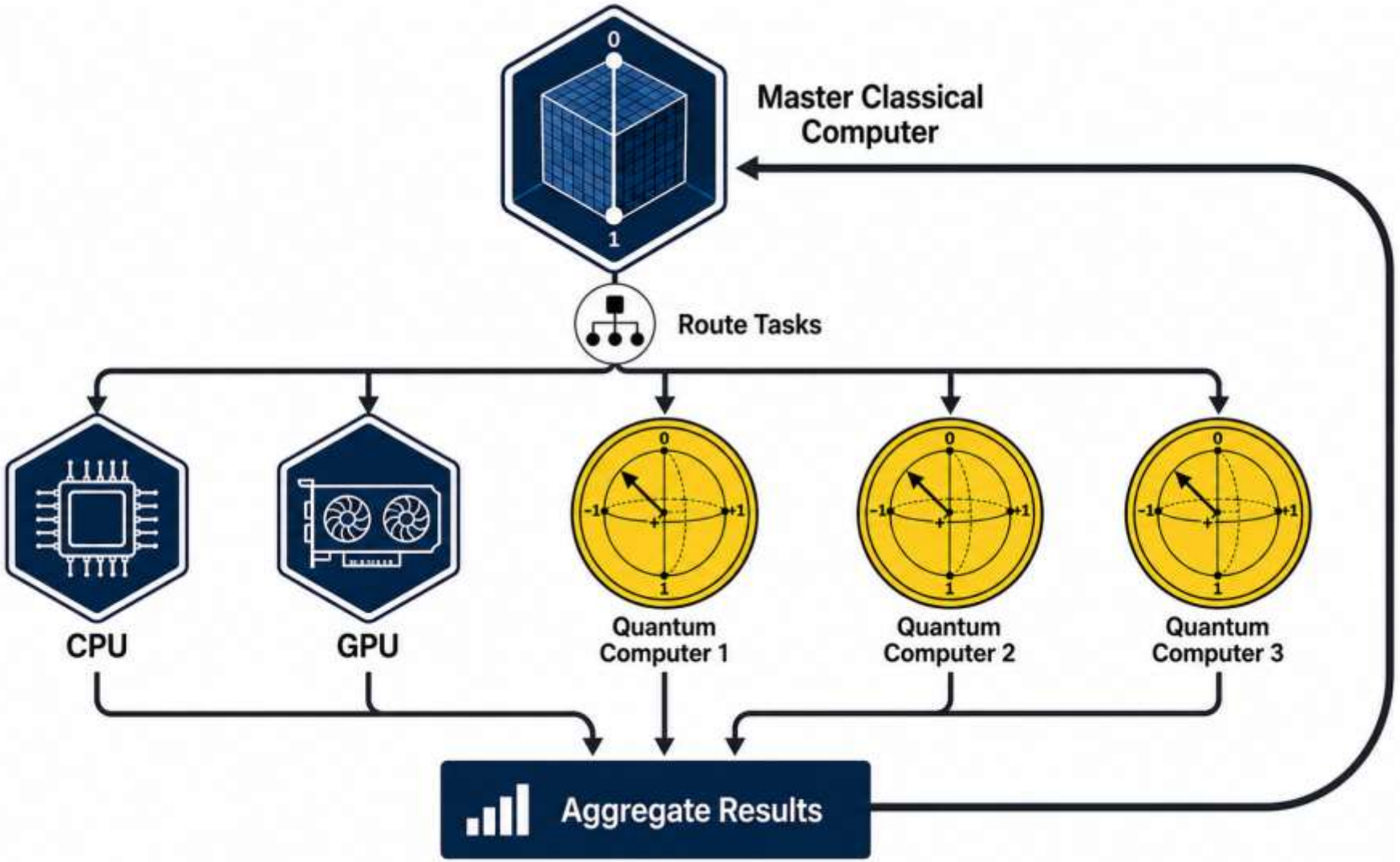
Alg. ECC-256 (this work)
Alice & Bob
Neutral-atom

Dallaire (April 2026)

Current state of play

Area	Current position
Controlling physical qubits	🟢 Demonstrated
Specialised quantum advantage	🟢 Demonstrated
Small logical qubits	🟡 Emerging
Useful fault-tolerant algorithms	🟡 Early demonstrations
Broad commercial advantage	🔴 Not yet demonstrated
Large-scale fault-tolerant machines	🔴 Still under development

Future: Hybrid quantum-classical workflows



Quantum solutions to solve our biggest challenges

Capture nitrogen to secure food supply for a growing planet

Enable more efficient chemical processing and catalysis

Energy storage to decarbonize transportation

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Hermann	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

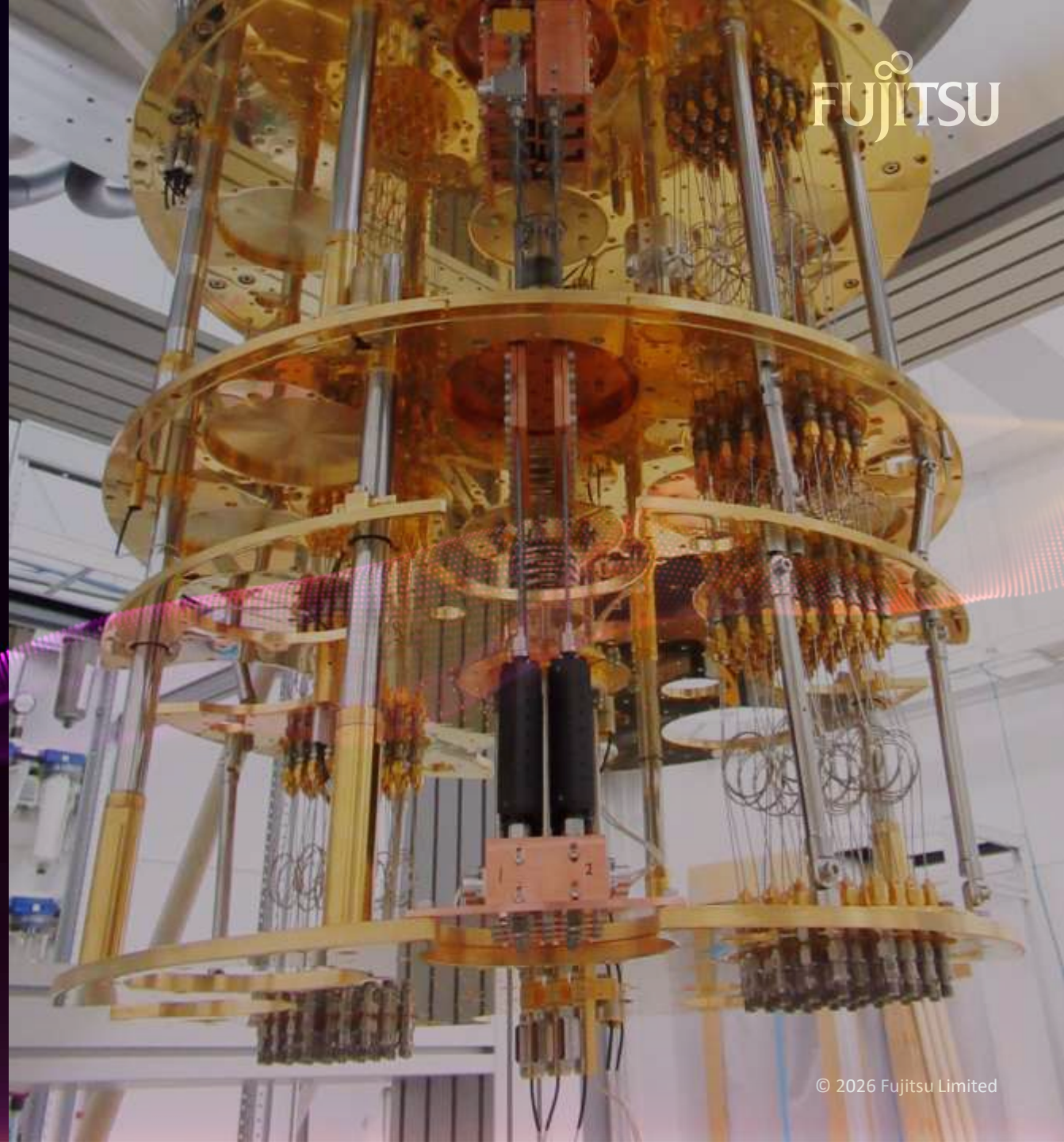
Actuaries Institute.

Quantum Computing for Actuaries

Ken Hermann

Go-To-Market Lead

Fujitsu



Agenda

- Quantum Advantages
- Timelines
- Quantum & AI
- Use cases

Quantum Computing: A quick primer

What it is, and why it speaks the same language as actuarial work

FUJITSU

What is it?

Computers that use qubits to explore many possibilities at once; a fundamentally different way to tackle certain problems

Why it’s hard

Qubits are fragile; today’s quantum systems are still small and error-prone, though fault tolerance is now being demonstrated

Why Actuaries?

The actuary field already spans uncertainty, risk, optimisation and long-run simulations; exactly where quantum aims to add value

Where it stands

Early but real: available today for research via cloud, improving fast, not yet ready for production decisions

The most immediate value isn't using a quantum computer - it's knowing which problems are quantum candidates.

The Power of Quantum Computing

FUJITSU

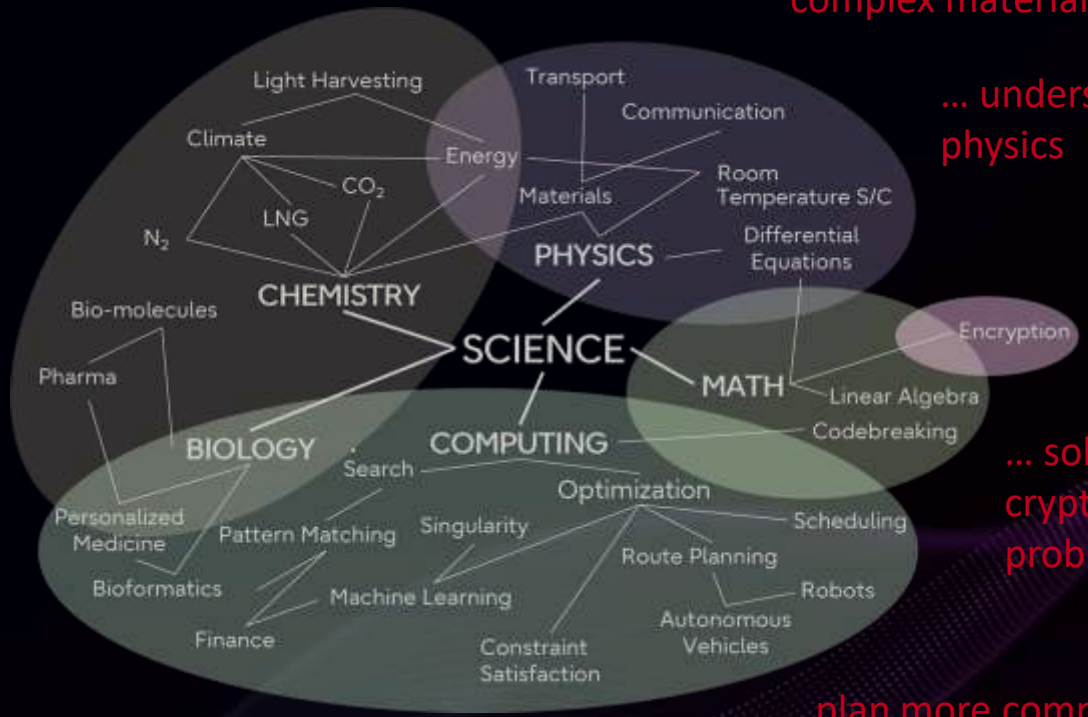
… better pharmaceuticals in shorter time

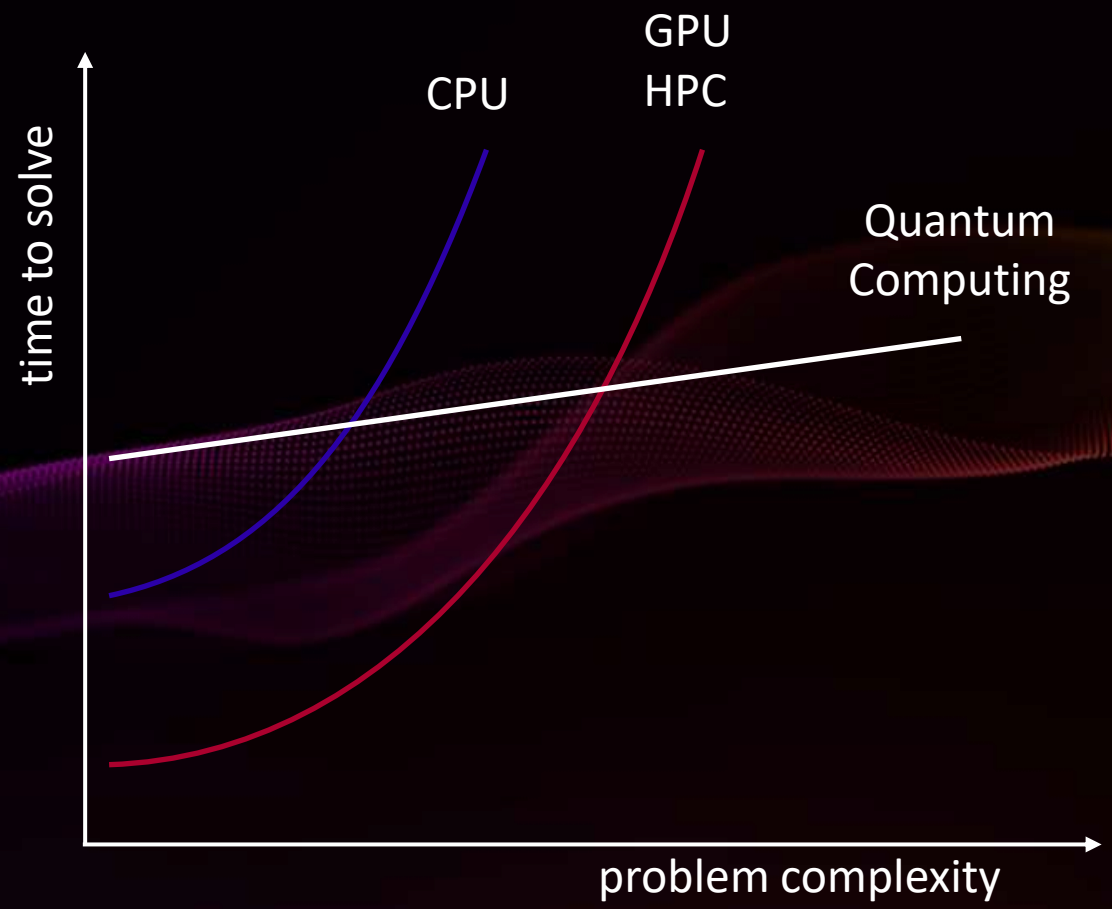
… simulate/discover more complex materials

… understand physics

… solve complex cryptographic problems

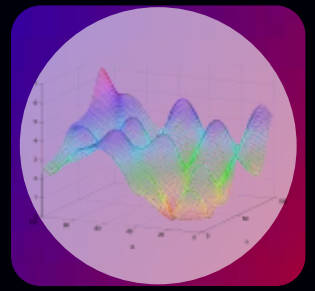
… plan more complex routing scenarios in shorter time





Quantum Computing Industry Network based on WEF Davos

What can we do with them?

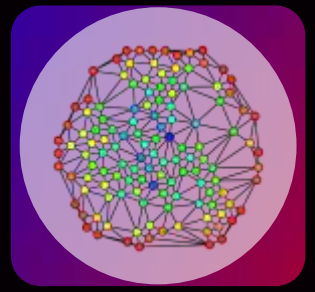


Simulations & models

- Weather & Climate risk modelling
- Computational fluid dynamics
- Material science
- Financial stock volatility
- Protein folding
- Drug discovery

Machine Learning Augmentation

- Fraud detection
- Data augmentation
- ML training synthetic data



Optimization models

- Portfolio & reinsurance optimisation
- Production line management
- Microgrid power balancing
- Last mile delivery
- JIT Logistics optimisation

Improved Security

- Quantum key encryption
- Quantum blockchain
- Quantum currency

Quantum streams – more than just compute

FUJITSU

Quantum Sensing

Uses quantum effects such as superposition and entanglement to detect magnetic fields, gravity, time, position, and motion.

E.g. Non-GPS navigation - underground

Timeline: 0 – 5 years

Quantum Communication

Uses quantum states (typically photons) to transmit information and cryptographic keys with the ability to detect eavesdropping.

E.g. Quantum key distribution

Timeline: 1 – 7 years

Quantum Computing

Uses qubits and quantum algorithms to solve certain optimisation, simulation, and scientific problems more efficiently than classical computers.

E.g. Drug discovery

Timeline: 5 – 10+ years

Quantum Computing Timelines

FUJITSU

What's accessible today?

- Quantum annealing for optimisation problem solving has been commercially available for 15 years (D-Wave)
- Quantum inspired Fujitsu Digital Annealer commercially available since 2018
- Real NISQ gate-based quantum hardware accessible for research as a pay-as-you-go from cloud hyperscalers
  - No capital investment required
- The future of compute is a combination of HPC, AI and Quantum Computing, typically on the cloud.

Evolution toward Next-Generation Computing

FUJITSU

2023
NISQ
Accelerating the development of quantum applications

2030
Early-FTQC
Realizing practical quantum computing (※)

2040
FTQC
Unleashing the true potential of quantum computers

※In some areas where supercomputers are not practically able to solve problems

Computation scale: high

Drug discovery
Material
Finance
Quantum for AI
CAE/CFD

Practical quantum computation

Quantum computing


64 qubits


Quantum simulator


256 qubits

Diamond spin


1,024 qubits


STAR Architecture


10,000+ qubits
(250 logical qubits)


1,000 logical qubits

Evolving through the integration of different technologies

Integrated HPC - AI - Quantum Computing

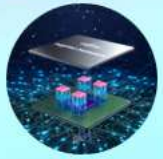
Quantum-inspired computing / AI

Digital Annealer
As-a-Service

Conventional Computing


HPC
FX1000

Processor
A64FX


Processor
FUJITSU-MONAKA
2nm


Processor
FUJITSU-MONAKA-X
1.4nm


Processor
FUJITSU-MONAKA-XX
cutting edge process node

Fujitsu Quantum Computer Roadmap

FUJITSU

FY 2022 | 2023 | 2024 | 2025 | 2026 | 2030 | 2035

March
36 -qubit Simulator

March
Helped RIKEN release first Japanese domestic quantum computer

July
40 -qubit Simulator

October
64 -qubit quantum computer
Developed by RIKEN RQC – Fujitsu Collaboration Centre

August
Establishment of high-speed execution method of practical algorithm using original quantum computing technology STAR architecture

March
256 -qubit quantum computer
Computer with quantum-classical hybrid applications

December
1,024 -qubit quantum computer

10,000+ -qubit (250 logical qubits) quantum computer

1,000 -logical qubit quantum computer

PRESS RELEASE

Fujitsu starts official development of plus-10,000 qubit superconducting quantum computer targeting completion in 2030

Development activities to be carried in part under NEDO project to advance the development of quantum computers towards industrialization

Fujitsu Limited

Kawasaki, Japan, August 1, 2025

Fujitsu today announced that it has started research and development towards a superconducting quantum computer with a capacity exceeding 10,000 qubits. Construction is slated for completion in fiscal 2030.

The new superconducting quantum computer will operate with 250 logical qubits and will utilize Fujitsu's innovative "STAR architecture," an early-stage fault-tolerant quantum computing (early-FTQC) architecture also developed by the company. Fujitsu aims to make practical quantum computing possible, particularly in areas like materials science where complex simulations can unlock groundbreaking discoveries, and to this end will focus on advancing key scaling technologies across various technical domains.

https://global.fujitsu/en-global/newsroom/gl/2025/08/01-01-en

September 2025
Completion of quantum building

December 2026
1,024 -qubit machine
×HPC(**FUJITSU-MONAKA**)
Hybrid calculation center

2031
10,000+ -qubit machine
×HPC
(**MONAKA-X, GPU servers**)
Hybrid calculation center

Quantum Computing Challenges

FUJITSU

Quantum Application	Need to find the right problem to solve Quantum algorithms for applications
Quantum Software	Quantum Computer control software Quantum algorithms for error correction
Quantum Platform	Middleware Compiler
Quantum State Control **Quantum Device & Integration**	Need excellent control of fragile quantum systems Need very well isolated qubits (low pressure, low temperature)

AI is helping to mitigate these challenges

The Quantum-AI Intersection

FUJITSU

AI → Quantum

Making Quantum usable today

- AI optimises quantum hardware design, build and operation
- Machine learning used to support gate-optimization, error-correction and hardware calibration
- Discovery of new quantum experiments and algorithms
- AI makes quantum less dependent on scarce quantum specialists

Quantum → AI

Accelerating AI

- Quantum can potentially accelerate AI training and optimisation, and help AI systems analyse far larger, higher-dimensional datasets
- Creation of complex, high-dimensional synthetic training data for ML
- Quantum advantage on mainstream AI training is a 'watch closely' technology

Quantum won't replace AI, and AI won't make quantum obsolete. The near-term reality is hybrid - classical deep learning with quantum support.

Fujitsu Quantum-AI Hybrid – Example

FUJITSU

Quantum + AI for catalyst discovery

Framework that integrates quantum algorithms with optimisation / AI techniques into business workflows for computational chemistry problems.

Business problem Complex catalyst surface modelling and molecule adsorption simulation are difficult for current computers, driving costly physical experimentation.

1. Candidate catalyst surface

Model molecular patterns on complex surfaces

2. Quantum algorithm layer

Use Quantum Fourier transform to model surface patterns

3. AI / optimisation layer

Calculate adsorption energy via combinatorial optimisation

4. Decision output

Prioritise catalyst candidates for investigation

Expected value

Quantum-enabled searches for complex catalysts difficult to analyse today.

Fujitsu differentiation

Quantum, HPC, ML and optimisation coordinated into practical workflows.

Case examples cited: CeO_2 catalysts (La-doped) | PdZn catalysts

Quantum Computing Use Cases for Actuaries

FUJITSU

Actuary work includes exactly the kinds of complex probabilistic and optimisation problems quantum is being designed to help solve

1 Hyper-granular, real-time pricing

Incorporate telematics, smart-building and wearable IoT data into pricing, moving beyond broad actuarial tables toward individualised risk pricing.

2 Catastrophe & climate risk modelling

Model cascading impacts from fires, storms and floods, where classical models struggle to capture full dimensionality.

3 Faster, richer Monte Carlo simulation

Speed up and refine simulations actuaries already depend on, as model complexity outpaces classical computational limits.

4 Portfolio & reinsurance optimisation

Early quantum algorithms are being tested against core problems across non-life, life insurance and reinsurance structuring.

5 Cryptographic & long-tail data risk

Encryption protecting today's claims and policy data may be breakable by future quantum computers - a live governance issue given decades-long data lifespans.

WHY IT MATTERS

Quantum offers a path from approximate models to high-fidelity, granular simulation.

Monte Carlo simulation for actuarial risk

FUJITSU

Current classical Monte Carlo

Brute-force sampling: more precision requires many more paths

1 → 2 → 3

Inputs
Policies, claims, market, longevity, catastrophe assumptions

Paths
Iteratively run many independent stochastic scenarios on HPC / cloud

Risk outputs
Mean, tail loss, VaR/TVaR, solvency capital and pricing

Hybrid classical + quantum Monte Carlo

Classical model orchestration + quantum amplitude estimation subroutine

1 → 2 → 3 → 4

State Preparation
Prepare a superposition of all stochastic scenarios according to inputs and probability distribution

Quantum Oracle
Estimate expected loss amplitude with fewer oracle calls

Amplitude Estimation
Estimate expected loss amplitude with fewer oracle calls

Measurement
Classical post-process to convert estimate into actuarial risk measures and scenarios

Scale of Quantum advantage

Example: 1,000,000 stochastic paths → **~1,000 quantum circuit evaluations**

Comparing the Compute Approaches for Monte Carlo

Four ways to run or accelerate the same simulation — each with a different maturity and risk profile

	Classical Compute	Digital Annealer	Quantum Annealing	Gate-Based Quantum
HOW IT WORKS	Direct random sampling on CPU/GPU — today's standard actuarial approach	Hardware-accelerated simulated annealing (MCMC) on a classical CMOS chip; mimics tunneling in software	Real qubits physically evolve via quantum tunneling to sample low-energy states	Quantum amplitude estimation on superposed states — direct analogue to classical Monte Carlo sampling
EXPECTED SPEEDUP	Baseline (1x)	~10–100x vs. classical (benchmarked)	~1–10x vs. classical	Theoretical 1,000 quadratic speedup (up to ~10,000x at high precision)
AVAILABILITY TODAY	Universal, fully mature	Commercially available since 2018 (Fujitsu)	Commercially available since 2011 (D-Wave)	Cloud access today; not yet at production scale
PROS	Flexible, well understood, no reformulation needed	Fast, no quantum noise, production-ready today	Genuine quantum tunneling may escape deep local minima classical methods miss	Only approach with a proven speedup for general MC/integration problems
CONS	Cost grows sharply for high-precision tail estimates	Limited to QUBO-style optimisation/sampling problems	No proven general advantage yet; only suits problems mappable to Ising form	Needs deep, coherent circuits — blocked by today's fault-tolerance limits

Source: Fujitsu Digital Annealer benchmarks (arXiv 2303.08392), D-Wave Leap, Montanaro (2015), arXiv 2607.10772 (Jul 2026)

Key take aways

FUJITSU

Quantum readiness starts before quantum advantage

- The most immediate actuarial value is not using a quantum computer - it is knowing which problems are quantum candidates.
- Actuaries are well positioned because your field already spans uncertainty, risk, optimisation, simulation and long-term capital decisions.
- AI is accelerating quantum usability today - quantum may later accelerate selected AI and modelling workloads.
- The prudent path is experimentation, risk assessment and ecosystem engagement — especially around optimisation, simulation and post-quantum cyber risk.

Call to action

- Start identifying use cases and testing in simulators
- Increase your awareness of quantum speedup and post-quantum risk

Thank you

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Herman	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

Actuaries Institute.

QUANTUM THREAT TO QUANTUM ADVANTAGE:
SECURING THE FUTURE OF FINANCIAL INFRASTRUCTURE

Quantum Insight Session 2026

Andreas Baumhof
QUINTESSENCELABS, CTO

Quantum will fix everything

ASICS QUANTUM Sneakers

QUANTUM RISK IS A FINANCIAL REALITY

- **Finance is uniquely exposed** – Cryptography underpins payments, identify and trust- failure at any layer can halt the system
- **The threat is already active** – “Harvest Now, Decrypt Later” (HNDL) attacks means sensitive financial data is being collected today for future compromise
- **This is not a standards problem** – Post-quantum algorithms exist – the challenge is deploying them across large, complex ecosystems
- **This is a systemic transition** – Cryptography is embedded everywhere

The shift is clear: quantum is no longer a future technology issue … it directly challenges today’s foundation of financial stability.

THE SCALE OF THE SHIFT

FROM CRYTPOGRAPHIC TRANSFORMATION → TO SYSTEMIC FINANCIAL RISK

Quantum computing will trigger the **largest upgrade of cryptography in human history,** far bigger than Y2K.

– *Steve Suarez, CEO of HorizonX & Sr Advisor, McKinsey & Company*

McKinsey & Company

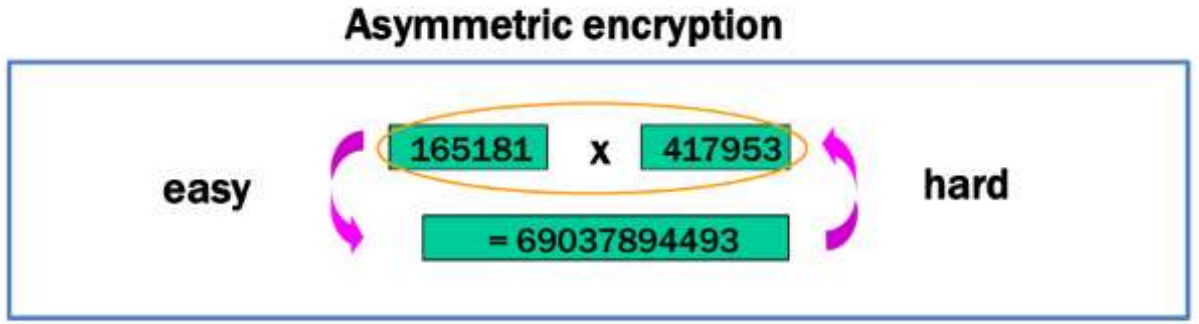
A single disruption to Fedwire could put **$2.0–$3.3 trillion** of US GDP at risk—in just one day.

– *Citi Institute, "Quantum Threat: The Trillion-Dollar Security Race Is On" - Jan 2026*

citi

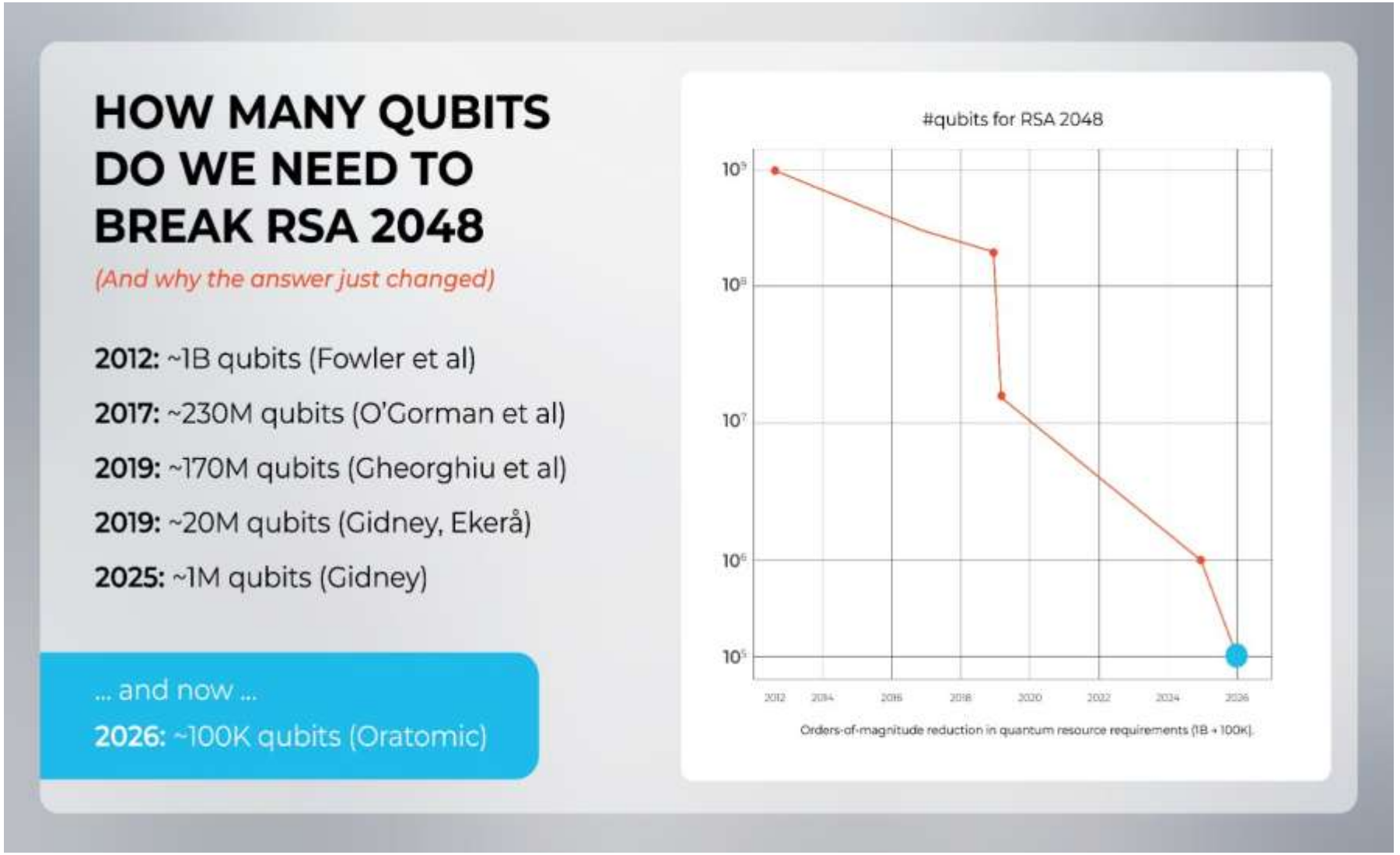
Shor’s algorithm

Shor's algorithm (1994) – a quantum algorithm that factors integers exponentially faster than classical methods, revolutionizing quantum computing and challenging modern cryptography.

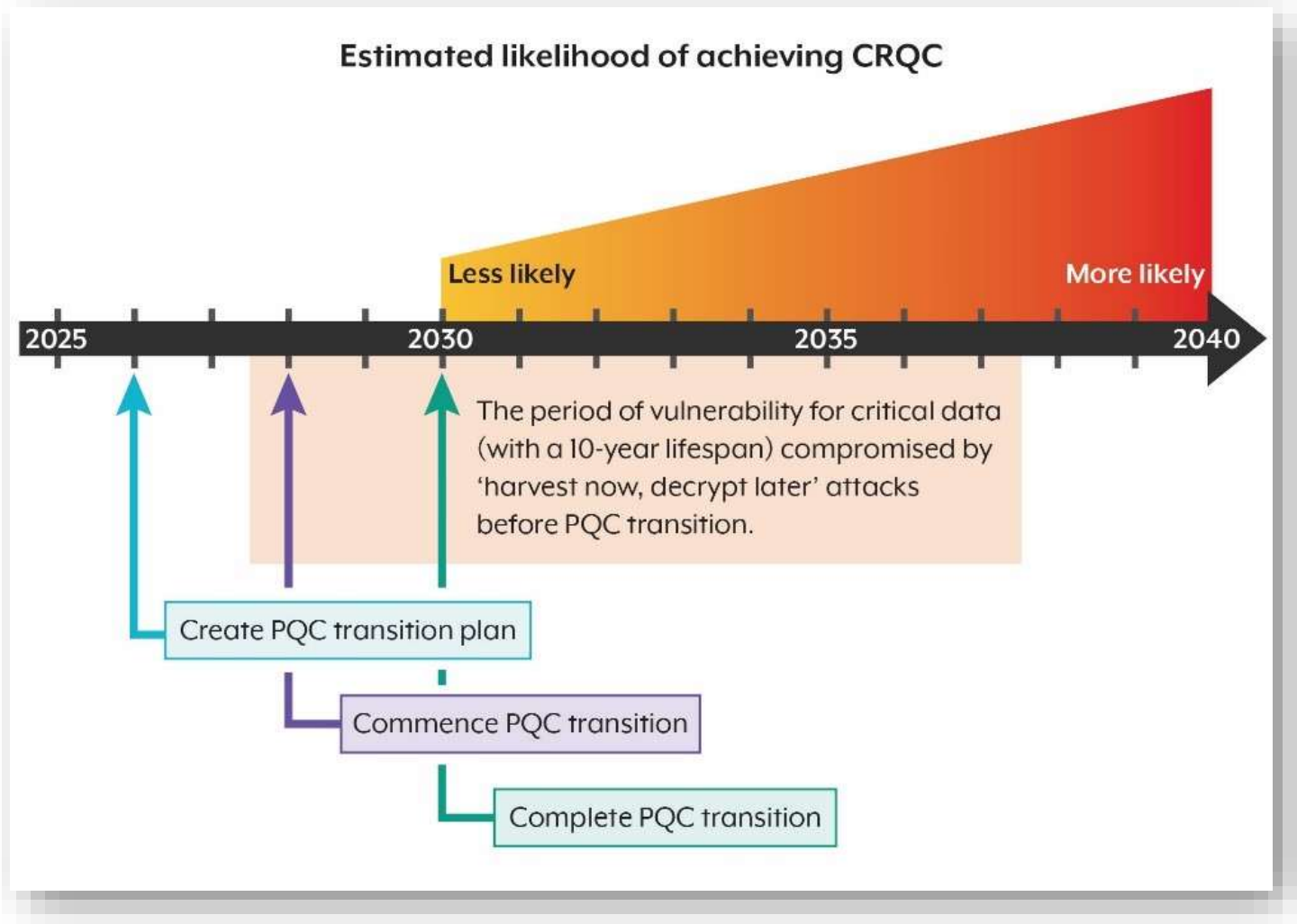


FROM 1B → 100K QUBITS

- Recent advances in quantum algorithms and architectures are rapidly reducing the resources required to break RSA-2048
- The implication is clear — the timeline to cryptographic risk is compressing and preparation windows are narrowing



ASD ASSESSMENT OF THE THREAT



https://www.cyber.gov.au/business-government/secure-design/quantum/planning-for-post-quantum-cryptography

ADDRESSING CURRENT AND POST-QUANTUM SECURITY NEEDS.

POST-QUANTUM ALGORITHMS INTEGRATION

Understand and evaluate NIST's post-quantum encryption standardization

CISO migration strategy and journey to quantum-resistant cryptography

Third party vendor implementation versus in-house development

QUANTUM RESISTANT ALGORITHMS

ENTERPRISE KEY MANAGEMENT AT SCALE

Efficient quantum-enabled management of and approach to encryption, signatures, and certificates

Speed and flexibility to rapidly adjust in response to new security incidents, threats, and regulatory compliance

CRYPTO AGILE KEY MANAGEMENT

TRUE RANDOM NUMBER GENERATION

Strengthen security of high-value long-lived digital assets and critical systems

Highest security seed content generated through the effect of quantum physics and not math

Ability to continuously monitor entropy source health

QUANTUM ENTROPY SOURCE

QUANTUM SECURE COMMUNICATION LINK

Need for a provably secure cryptographic building block – quantum safe key distribution – for remote parties to share cryptographic keys

Ability to detect and address attacks on communication link(s) in real-time

QUANTUM SAFE KEY DISTRIBUTION

CRYPTO-AGILE POST-QUANTUM-CRYPTOGRAPHY PLATFORM

- Crypto Discovery
- Crypto Management Engine (symmetric and asymmetric)
- Separation of application logic from crypto logic
- Policy based crypto configuration

https://blog.google/innovation-and-ai/te...

Chat

Google The Keyword

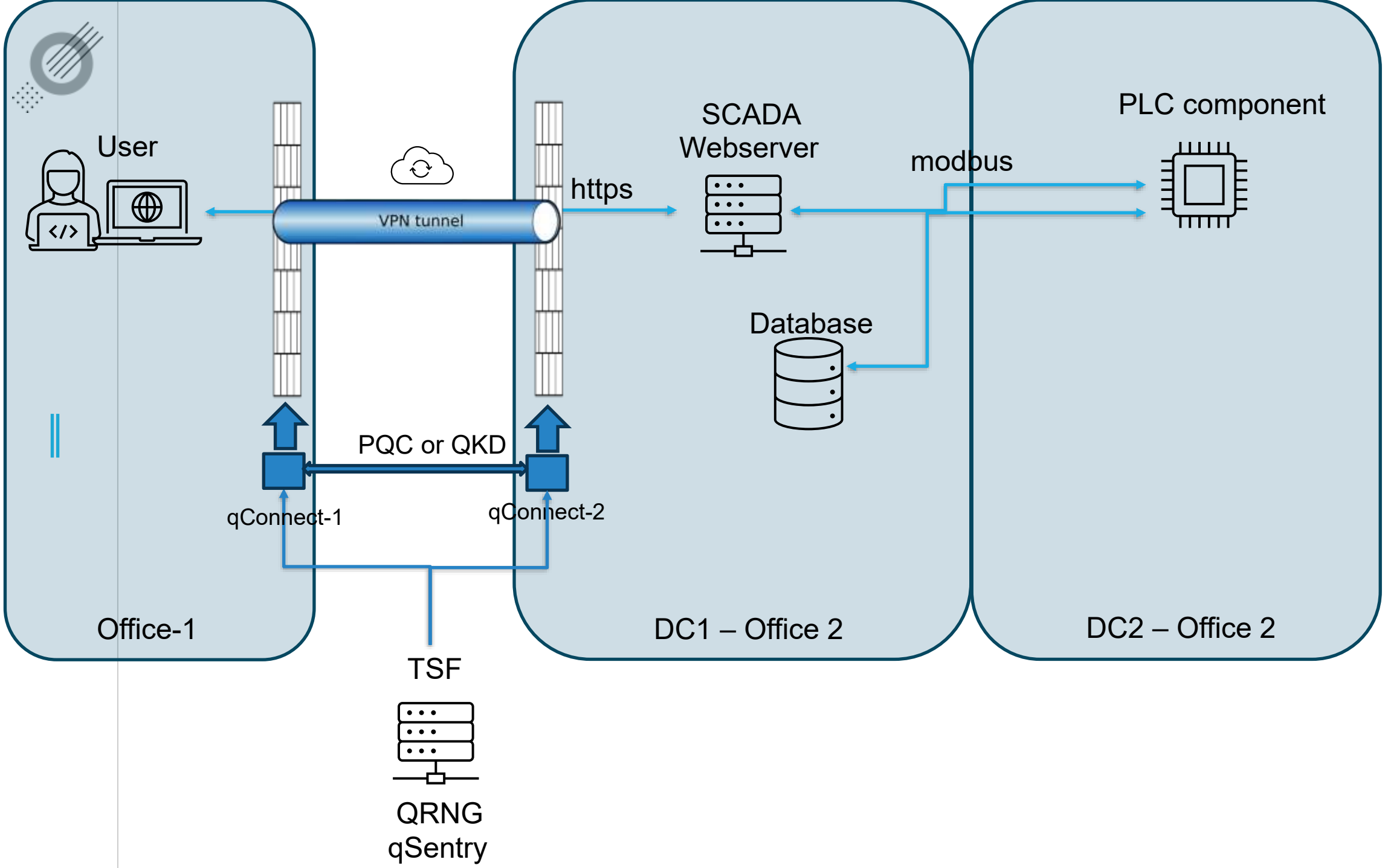
INNOVATION & AI > TECHNOLOGY > SAFETY & SECURITY

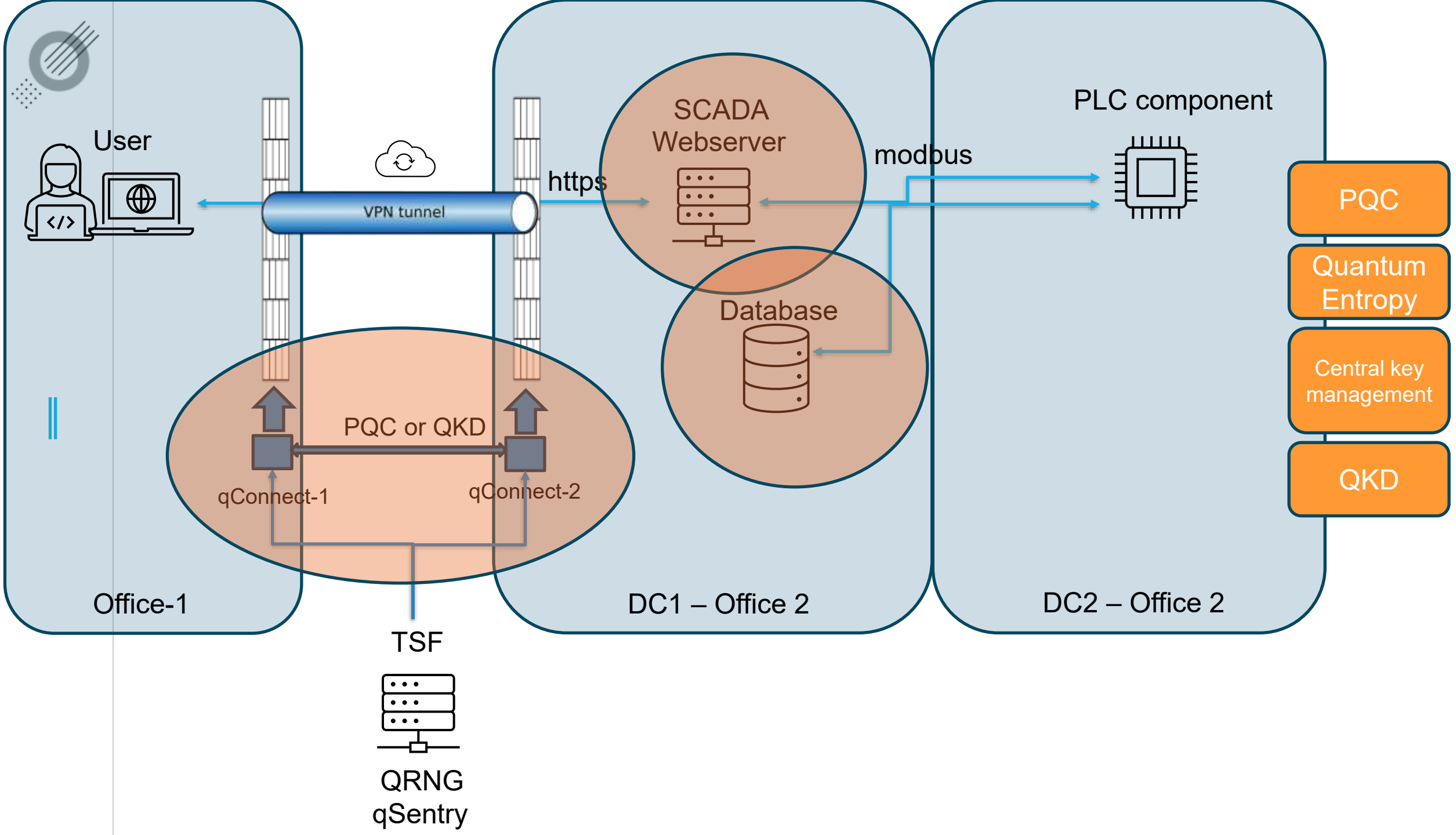
Quantum frontiers may be closer than they appear

Mar 25, 2026 · 2 min read

Share

We're setting a timeline for post-quantum cryptography migration to 2029.

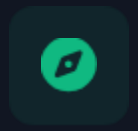

User
VPN tunnel
https
SCADA
Webserver
modbus
PLC component
Database
PQC or QKD
qConnect-1
qConnect-2
Office-1
DC1 – Office 2
DC2 – Office 2
TSF
QRNG
qSentry


User
VPN tunnel
https
SCADA
Webserver
modbus
PLC component
Database
PQC or QKD
qConnect-1
qConnect-2
PQC
Quantum
Entropy
Central key
management
QKD
Office-1
DC1 – Office 2
DC2 – Office 2
TSF
QRNG
qSentry

Quantum is Only the Trigger. Agility is the True Objective.

- Quantum computers may be the ultimate catalyst driving modern regulatory pushes, but they are far from the only threat facing classical cryptography today.
- From shortened digital certificate lifespans (dropping to 47 days by 2029) to rapid cloud-based brute-forcing and newly discovered zero-days, algorithms are decaying faster than ever before.
- To survive, enterprises must decouple core application logic from the underlying mathematical ciphers.

Four Pillars of Crypto-Agility



Discovery

Continuous discovery and continuous inventory of metadata for every key, certificate, and library in use.

Abstraction

Isolating core data encryption functions from underlying math using abstract cryptographic service APIs.

Policy

Centralizing cryptographic controls so changes can be enforced instantly without redeploying code.

Automation

Orchestrating lifecycle processes including automated rotation, testing, and secure algorithm rollback.

The Cost of Deferred Agility

"Waiting doesn’t delay cost,
it concentrates risk."

— Gartner Executive Briefing

The risk is we do little or nothing ... **until we are forced to!**

⚠ **SECURITY WARNING: CONCENTRATED TIMELINES GUARANTEE OPERATIONAL FAILURE**

Qlabs PQC Readiness Assessment

Assessment Methodology

Software-Driven Discovery: Automated scanning service utilizing specialized technology to generate an initial **CBOM**.

Interactive Workshops: Structured engagement with key stakeholders to document current status-quo and operational workflows.

TSF Sentry Framework: Risk-based, crypto-agile remediation framework ensuring future cipher changes are handled via *simple policy changes*.

Audit-Ready Report for Regulatory Entities & Compliance

PQC Readiness Report Deliverables

1. CBOM Inventory Report
Visibility into cryptographic applications, algorithms and dependencies.

2. High-Level PQC Risk Assessment
Prioritized vulnerability mapping based on workshop findings and threat exposure.

3. Remediation Plan & Status
Actionable roadmap to showcase tangible progress to regulatory bodies and governance boards.

THANK YOU

Andreas Baumhof
ab@quintessencelabs.com

www.quintessencelabs.com

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Hermann	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

Actuaries Institute.

Agenda

• Dr Anthony Lowe	Introduction
• Rishi Krishanasamy	National mandate and why quantum matters for industry
• Dr Maja Cassidy	Quantum 101
• Ken Hermann	Quantum advantages, timelines , Quantum & AI, use cases
• Andreas Baumhof	Quantum threat to quantum advantage
• Mark Griffiths	Actuaries Institute quantum computing working group
• Q&A	

Actuaries Institute.

Q&A

Join at
slido.com
#2008252

Feedback Poll

Join at
slido.com
#2008252